THE UNIVERSITY OF SYDNEY

COPYRIGHT AND USE OF THIS THESIS

This thesis must be used in accordance with the provisions of the Copyright Act 1968.

Reproduction of material protected by copyright may be an infringement of copyright and copyright owners may be entitled to take legal action against persons who infringe their copyright.

Section 51 (2) of the Copyright Act permits an authorized officer of a university library or archives to provide a copy (by communication or otherwise) of an unpublished thesis kept in the library or archives, to a person who satisfies the authorized officer that he or she requires the reproduction for the purposes of research or study.

The Copyright Act grants the creator of a work a number of moral rights, specifically the right of attribution, the right against false attribution and the right of integrity.

You may infringe the author's moral rights if you:

- fail to acknowledge the author of this thesis if you quote sections from the work
- attribute this thesis to another author
- subject this thesis to derogatory treatment which may prejudice the author's reputation

For further information contact the University's Director of Copyright Services

sydney.edu.au/copyright

Algorithms for Galois Extensions of Global Function Fields

Nicole Sutherland

A thesis submitted in fulfillment of
the requirements for the degree of
Doctor of Philosophy

Pure Mathematics
University of Sydney

May 2015

Abstract

In this thesis we consider the computation of integral closures in cyclic Galois extensions of global function fields and the determination of Galois groups of polynomials over global function fields. The development of methods to efficiently compute integral closures and Galois groups are listed as two of the four most important tasks of number theory considered by Zassenhaus [**Poh94**].

We describe an algorithm each for computing integral closures specifically for Kummer, Artin–Schreier and Artin–Schreier–Witt extensions. These algorithms are more efficient than previous algorithms because they compute a global (pseudo) basis for such orders, in most cases without using a normal form computation. For Artin–Schreier–Witt extensions where the normal form computation may be necessary we attempt to minimise the number of pseudo generators which are input to the normal form. These integral closure algorithms for cyclic extensions can lead to constructing Goppa codes, which can correct a large proportion of errors, more efficiently.

The general algorithm we describe to compute Galois groups is an extension of the algorithm of [**FK14**] to polynomials over function fields of characteristic p. This algorithm has no restrictions on the degrees of the polynomials it can compute Galois groups for. Previous algorithms have been restricted to polynomials of degree at most 23. Characteristic 2 presents additional challenges as we need to adjust our use of invariants because some invariants do not work in characteristic 2 as they do in other characteristics. We also describe how this algorithm can be used to compute Galois groups of reducible polynomials, including those over function fields of characteristic p.

All of the algorithms described in this thesis have been implemented by the author in the Magma Computer Algebra System [**CBFS13**] and perform effectively as is shown by a number of examples and a collection of timings.

Acknowledgements

Thank you to the anonymous referees of my reviewed papers for their suggestions.

I would like to thank Claus Fieker for his supervision throughout my candidature, even by distance after his relocation, and his hospitality during two visits in which I worked on aspects of this thesis.

Thank you to Stephen Donnelly for supervising me after Claus' relocation.

Thank you to John Cannon for having me as part of the Computational Algebra Group throughout my candidature and allowing me to include my implementations in Magma.

Thank you to Allan Steel, Geoff Bailey and David Howden for advice on and help with many practical matters. Thank you to William Unger for advice on Group theory and to Andreas-Stephan Elsenhans for discussions about Galois group computations.

Thank you to my husband David for his encouragement to begin and finish this thesis.

Declaration

To the best of my knowledge, this thesis contains no material previously published by any other person except where due acknowledgement has been made.

Contents

Introduction

In this thesis we consider some computational problems in Galois extensions of global function fields. In particular we investigate the efficient computation of integral closures in cyclic extensions of global fields and the computation of Galois groups for polynomials over global function fields.

Function fields have been studied since the 19th century when they were investigated by Dedekind, Kronecker and Weber. They were further considered by Artin, Hasse, F. K. Schmidt and Weil in the 20th century and continue to be of interest because they provide a basis for designing efficient algorithms for the study of the geometry of algebraic curves. The study of a function field is equivalent to the study of a curve and so function fields can be studied from the algebraic geometry point of view. Applications of curves and function fields arise in coding theory and cryptography. Codes can be constructed from curves with some curves being more suited to this use than others. For efficient construction of codes from curves, or equivalently function fields, computations in the curves or function fields need to be done efficiently.

However, global function fields are analogous to number fields in that they are finite separable extensions of a rational function field in the same way that a number field is a finite extension of the rational field. In this thesis we consider function fields from the number theory point of view, as we take advantage of algorithms described for number fields which can be used similarly for function fields. Such algorithms can be found in [**Coh00**] where algorithms in [**Coh93**] are generalized to relative extensions of number fields. The generalization of these algorithms to global function fields can be done by analogy. This thesis uses these algorithms for global function fields including relative extensions of global function fields. We state our algorithms in as much generality as possible so that it is irrelevant whether the field is a number or function field and whether it is represented as a direct extension of the rational (function) field or not.

There are some tasks which have a rich history for number fields but have only recently sparked interest for function fields. These include the development of methods to efficiently compute integral closures, Galois groups, class groups and unit groups. The integral closure

in a field extension is an analogue of $\mathbb{Z}$. Such rings can be used in computing class groups, unit groups and Galois groups. The unit group computed from a field extension is the unit group of an integral closure in the field extension, indeed the unit group of the field itself is trivial. These tasks are listed as the four tasks of number theory which Zassenhaus considered most important [**Poh94**]. Zassenhaus contributed to each of these tasks but we note here especially his contribution to the computation of integral closures in the development of the Round 2 algorithm.

For function fields we are also interested in computing Riemann–Roch spaces of divisors or at least the dimension of such and computing the genus, the most important invariant, of a function field. The genus of a function field can be used to bound the difference between the degree and the dimension of all divisors of a function field. Divisors of a function field can be represented by ideals of integral closures in the function field and a calculation of bases for Riemann–Roch spaces can use this representation. The genus of a function field can be computed using the degree of the different divisor, the degree of the field extension and the relative degree of the algebraic closure of constant field in the extension. The algebraic closure of the constant field in the function field is equivalent to the Riemann–Roch space of the zero divisor. The genus can be used in the computation of the divisor class group of a function field, analogous to the class group of a number field. A method for calculating Riemann–Roch spaces of divisors and a method for computing divisor class groups of function fields is presented in [**Heß99**]. Improving the efficiency of the computation of integral closures can improve the computation of the genus, Riemann–Roch spaces and divisor class groups.

Function fields defined over a finite field k (with characteristic $p > 0$) are *global fields* along with number fields. Both these types of global fields have a class field theory which allows abelian extensions, that is, Galois extensions whose Galois group is abelian, to be classified completely. Class field theory has been studied since the beginning of the 20th century and prior to 1940 it was first considered also for global function fields by F. K. Schmidt and Witt ([**Ser88**] p. 159). Abelian extensions allow us to construct families of fields where we can control the genus and the number of rational places and allow a representation from which we can compute these values for such extensions relatively cheaply. However, in order to use these fields explicitly and compute the rational places themselves we need to be able to compute integral closures in these fields.

The construction of an Algebraic–Geometric code from a function field involves the computation of some rational places of the function field, the construction of a divisor,

the computation of a basis for its Riemann–Roch space and the evaluation of this basis at the rational places. Equivalently these codes can be constructed from divisors of a curve over a finite field. One of the core invariants of a code, its minimum distance, is linked to the genus and the number of rational places of the function field used to construct the code. How class field theory can be used to generate curves with many rational points compared to their genus is explained by Ducet and Fieker in [**DF12**]. This is motivated by the interest in finding linear block codes having high minimum distance compared to their block length. Algebraic–Geometric codes are of interest because curves having many rational points tend to have high minimum distances.

Efficient algorithms for computing integral closures in cyclic extensions of global function fields makes possible a wider range of applications. For example, this allows the construction of Algebraic–Geometric codes from much larger cyclic field extensions. Since a divisor can be constructed using integral closures in the function field the construction of the code benefits from improved efficiency in the integral closure computation.

Recent algorithms to compute integral closures or maximal orders in global fields include Round 2 (described in [**Coh93**]) and algorithms using local factorization [**Pau01, GMN11, GMN12, GMN13, Bau14**]. To gain a more efficient algorithm for cyclic extensions of number fields special techniques have been investigated by Daberkow in [**Dab95**]. Cyclic extensions of function fields were more recently considered by Fraatz in [**Fra05**]. Both of these techniques use the special shape of the defining polynomial to write down local generators at each prime of interest, at least one for each ramified prime. These generators each define an order which is P-maximal for a prime P. But these generators need to be combined to compute a global order. This combination of P-maximal orders for each prime of interest dominates the runtime of these approaches. To combine the P-maximal orders defined by these generators we need to essentially compute the smallest order containing all the P-maximal orders and this involves the computation of a normal form to compute a basis for the global order. So while these approaches describe maximal orders in theory, in practice the construction of the orders themselves is expensive.

In cyclic extensions the combination of the local maximal orders can be done efficiently and a (pseudo) basis can be written down directly for the global maximal orders. This can be done without calculating local generators but by using the ideals in the pseudo bases the P-maximal orders can be combined efficiently. By calculating a basis for the maximal orders "by hand", which we show can be easily done, we save much computation time in computing a basis from generators. The special shape of the defining polynomials

means that in many cases we can avoid any normal form computations which has not been avoided in previous algorithms. It is possible to do this for cyclic extensions because the special shape of the polynomials involved allows a special relationship between the constant coefficient and the discriminant of the polynomial and also between the constant coefficient and the primitive element of the extension. Additionally, we compute integral closures without computing any other subrings of the function field as the Round 2 method does and without factoring (or sometimes even computing) the discriminant of the defining polynomial.

This thesis is structured as follows. Chapter 1 contains background information about orders as a type of subring of function fields. The details regarding our efficient algorithm for computing integral closures in Kummer extensions (more generally, radical extensions) are found in Chapter 2. Here we have been able to compute a diagonal basis for the integral closures. We describe efficient algorithms for computing integral closures in Artin–Schreier–Witt extensions in Chapter 5 and for the simplest case of Artin–Schreier extensions in Chapter 3. In Artin–Schreier extensions we have been able to compute a triangular basis for the integral closures. In Artin–Schreier–Witt extensions we have been able to compute a (pseudo) basis for S-maximal orders where S contains primes of the same ramification degree, rather than generators corresponding to each individual prime. We also compute a basis for a degree p^n extension rather than the Artin–Schreier–Witt tower of n extensions of degree p as does [**Fra05**]. These cyclic extensions cover all possibilities for components of abelian extensions.

We will show that we have removed in practice one of the barriers to constructing good codes from cyclic extensions in Chapter 6.

Chapter 4 contains a short description of computing generators for prime ideals which extend totally ramified primes in a Kummer or Artin–Schreier extension using information presented in Chapters 2 and 3.

Since abelian and cyclic extensions are types of Galois extensions and computing Galois groups is also considered to be an important task of number theory, in Chapters 7, 8 and 9 we describe an algorithm to compute Galois groups of polynomials of unrestricted degree over global function fields. Since Stauduhar developed an interesting practical algorithm [**Sta73**] for the computation of Galois groups there have been a number of other algorithms described but these have mostly been specific to polynomials over the rational field. We consider in Chapter 7 the recent algorithm by [**FK14**] which removes the degree restriction of [**Gei03, GK00**] and also introduce computations of Galois groups. Chapter 8

expands on the algorithm in Chapter 7 and describes how we adjust this algorithm so that it can be used to compute Galois groups of polynomials over characteristic p function fields, including when the characteristic is 2 in which case replacement invariants were required. In theory [**Gei03**] applies to polynomials over fields of small characteristic but there have been found to be problems in practice with this approach. Additionally the algorithm we present to compute Galois groups of irreducible polynomials over characteristic p function fields is the first to use the computation of the subfields of the field extension defined by the polynomial. Most previous algorithms compute Galois groups of irreducible polynomials. We go further and compute Galois groups of reducible polynomials also. Chapter 9 explains how this algorithm can be used to compute Galois groups of reducible polynomials.

The main results of this thesis are the pseudo bases presented in Chapters 2, 3 and 5 and the details contained in Chapters 8 and 9. Most of the results in this thesis have been published in [**Sut12**], [**Sut13**] or [**Sut15**]. The results in Chapter 5 have been submitted for publication in [**Sut14**].

We have implemented our algorithms for integral closures in Magma [**CBFS13**] V2.16 (Chapters 2 and 3), V2.20 (Chapter 5) and later. Our algorithms for Galois groups have been implemented in Magma V2.16, V2.17 (Chapter 8) and V2.18 (Chapter 9) and later. For a discussion of function fields in Magma please see [**Fie06**].

Background and Notation

An *algebraic function field* is an extension field F containing a field k such that F is a finite algebraic extension of a *rational function field* $k(t)$ for some element $t \in F$ which is transcendental over k. A finite separable function field extension F'/F can be described by a *defining polynomial* f such that $F' = F[x]/f(x)$ or $F' = F(\alpha)$ where α is a root of f. The extension F'/F has *degree* $[F' : F] = \deg(f)$. The element α is a *primitive element* of F'/F and $\{\alpha^i\}_{0 \leq i < [F':F]}$ will be a basis for F'/F. A *subfield* $K \subseteq F'/F$ is a field extension K/F with $[F' : K][K : F] = [F' : F]$. The *algebraic closure* of F is an extension of F containing a root of every polynomial over F. The field k is the *constant field* of F and its algebraic closure in F we refer to as the *exact constant field* of F. These constant fields are *perfect* if all algebraic extensions of them are *separable*, that is, all irreducible polynomials over these fields have only distinct roots in an algebraic closure.

An *F-automorphism* of F'/F is an automorphism σ of F' such that $\sigma(a) = a$ for all $a \in F$. The *automorphism group* of F'/F is the group of all F-automorphisms of F', $\{\sigma : F' \to F' |\ \sigma$ is an isomorphism and $\sigma(a) = a\ \forall a \in F\}$. An algebraic extension F'/F is a *Galois extension* if the automorphism group of F'/F has order $[F' : F]$. The *Galois group* of a Galois extension is the automorphism group of the extension. A Galois extension of F is a *splitting field* for a separable polynomial f over F, a field containing all roots of f. The *normal closure* of F'/F is the minimal splitting field of the defining polynomial of F'/F over F.

A *place* P of an algebraic field F is the maximal ideal of a *valuation ring* $\mathcal{O}_P$, a proper subring of F containing the constant field of F such that $z \in \mathcal{O}_P$ or $z^{-1} \in \mathcal{O}_P$ for all $z \in F$. Since $\mathcal{O}_P$ is a local ring it has a unique maximal ideal so the place P is uniquely determined by $\mathcal{O}_P$ and $\mathcal{O}_P$ is uniquely determined by P ([**Sti93**] Section I.1). Since P is a principal ideal of $\mathcal{O}_P$, there is some *prime* or *uniformizing element* $\pi \in \mathcal{O}_P$ such that $P = \pi\mathcal{O}_P$. A place P has an associated valuation v_P defined by $v_P(z) = v_P(u\pi^n) = n, v_P(u) = 0$, a *residue class field* $\mathcal{O}_P/P$ and a *degree* $f_P = [\mathcal{O}_P/P : k]$. The *residue class map* or *evaluation map* at P takes an element a of $\mathcal{O}_P$ to the residue class $a + P$ of a modulo P. We denote the set of places of a field F by $\mathbb{P}_F$.

A *divisor* D of F is a formal sum of places of F, $D = \sum_{P \in \mathbb{P}_F} c_P P$ where only finitely many $c_P \in \mathbb{Z}$ are non zero. The *degree* of a divisor is $\sum c_P f_P$. The *principal divisor* of a non-zero element a is the divisor $(a) = \sum v_P(a)P$. A principal divisor has degree 0. A non-zero element a has a *zero* at P when $v_P(a) > 0$ and a *pole* at P when $v_P(a) < 0$. The principal divisor of a can be written as the difference between the *zero divisor* $(a)_0 = \sum_{\{P:v_P(a)>0\}} v_P(a)P$ and the *pole divisor* $(a)_\infty = \sum_{\{P:v_P(a)<0\}} -v_P(a)P$ of a. We have $0 = \deg((a)) = \deg((a)_0) - \deg((a)_\infty)$ so $\deg((a)_0) = \deg((a)_\infty)$.

The *Riemann–Roch space* of a divisor A of F is the vector space $\mathcal{L}(A) = \{x \in F^\times \mid (x) \geq -A\} \cup \{0\}$. The *dimension* of a divisor is the vector space dimension of the Riemann–Roch space of the divisor, over the exact constant field of F.

The *genus* of a function field is one more than the maximum difference between the degree of its divisors and their dimension.

When F' is a non trivial algebraic field extension of F, a place $P' \subset F'$ is said to *extend* $P \subset F$ if $P \subset P'$ for which we write $P' \mid P$. When $P' \mid P$, $\mathcal{O}_P \subset \mathcal{O}_{P'}$ and there is an integer $e(P'|P)$ such that $v_{P'}(z) = e(P'|P)v_P(z)$ for all $z \in F$ which we call the *ramification degree* of $P' \mid P$. The extension $P' \mid P$ is *ramified* if $e(P'|P) > 1$, *unramified* if $e(P'|P) = 1$ and the residue class extension $(\mathcal{O}_{P'}/P)/(\mathcal{O}_P/P)$ is separable and *totally ramified* if $e(P'|P) = [F' : F]$ in which case there is only one P' such that $P' \mid P$. The degree $f(P'|P)$ is the relative degree $[\mathcal{O}_{P'}/P' : \mathcal{O}_P/P]$. An unramified extension $P' \mid P$ is said to be *inert* if P' is the only ideal which extends P in which case the inertia degree $f(P'|P) = [F' : F]$ and *split* if there is more than one $P' \mid P$ and we have $f(P'|P) = 1$, $\forall P' \mid P$. In the simplest case we can compute these degrees by factoring the image of the defining polynomial of F'/F under the canonical extension of the residue class map at P to polynomials. The exponent of a factor is the ramification degree and the degree of a factor is the inertia degree of the corresponding ideal above P.

We consider the infinite place of a rational function field to be

$$P_\infty = \{g/h | g, h \in k[t], \deg(g) < \deg(h)\}.$$

We write $V_\infty = \{g/h | g, h \in k[t], \deg(g) \leq \deg(h)\}$ as the valuation ring of P_∞. The finite places of a rational function field $k(t)$ are then

$$P_\pi = \{g/h | g, h \in k[t], h \neq 0, \pi | g, \pi \nmid h\}$$

for irreducible polynomials $\pi \in k[t]$. The *finite* places of an algebraic function field $F/k(t)$ are those places of F lying above a finite place of $k(t)$ and the *infinite* places of $F/k(t)$

are those places of F lying above P_∞. We denote the finite places by $\mathbb{P}_F^0$, and the infinite places by $\mathbb{P}_F^\infty$.

Let a be an element of an algebraic function field F'/F. Then a has a *minimal polynomial*, a polynomial f_a of smallest degree over F such that $f_a(a) = 0$ and a *characteristic polynomial* of degree $[F' : F]$ which is the cth power of the minimal polynomial, $c = [F' : F]/\deg(f_a)$. The other roots of f_a in some algebraic closure are the *conjugates* $a^{(i)}, 0 \leq i < \deg(f_a)$ of a. The cth power of the product of the conjugates of a is the *norm* of a over F, $\mathrm{norm}(a)$ and the c times the sum of the conjugates of a is the *trace* of a over F, $\mathrm{Tr}(a)$.

An element a is *integral* over a subring R of F if there is a monic polynomial in $R[x]$ of which a is a root, in which case $v_P(a) \geq 0$ for all prime ideals $P \subset R$. If a is not integral over R then it will have a *denominator* ideal d_a with respect to R such that $d_a a$ is integral over R and $v_P(d_a a)$ is minimal for all prime ideals $P \subset R$. When $R \cap k(t)$ is a principal ideal domain, for example, $k[t]$ or V_∞, then there is an element $d_a \in R \cap k(t)$ such that $d_a a$ is integral and $v_P(d_a a)$ is minimal for all $P \subset R$. The set of elements of F which are integral over R is called the *integral closure* of R in F. A ring R is *integrally closed* if all elements of the field of fractions of R which are integral over R are in R. We denote by $\mathbb{Z}_F^0$ the integral closure of $k[t]$ in F and by $\mathbb{Z}_F^\infty$ the integral closure of V_∞ in F.

The *discriminant* of a polynomial f is $\mathrm{disc}(f) = \prod_{0<i\neq j\leq \deg(f)}(\alpha_i - \alpha_j)$ where α_i are the roots of f and can be computed as a resultant of f with its derivative, that is, without computing the roots of f.

A *localization* of a ring R at a place P is the ring $R_{R\cap P} = \{a/b : a, b \in R, v_P(b) = 0\}$. Since $R \subseteq R_{R\cap P}$ for each place P we have $R \subseteq \cap_P R_{R\cap P}$. When $P \subseteq R$ we can write R_P instead of $R_{P\cap R}$.

Let $d(a, b) = c^{-v_P(a-b)}$ for some constant $c > 1$ be a metric. A *completion* of a ring R at a place P is a ring in which all Cauchy sequences converge with respect to the metric $d(a, b)$ and for each element of the completion there is a Cauchy sequence in R which converges to it. It can be shown that completions of function fields are isomorphic to series rings. This isomorphism allows these completions to be implemented as series rings in MAGMA [**CBFS13**]. An element in a completion of a function field is a π-adic expansion of an element of the function field $a = \sum_{i=v_P(a)}^\infty a_i \pi^i, a_i \in \mathcal{O}_P/P$ at a uniformizing element π of P.

Part 1

Efficient Computation of Maximal Orders in Cyclic Extensions of Global Function Fields

Chapter 1

Function Fields and their Subrings

In the first part of this thesis we derive pseudo bases (see Definition 1.2) for S-maximal orders in cyclic extensions. The computation of orders from these pseudo bases is efficient and its complexity is linear in the degree of the field when the extension is Kummer, Artin–Schreier or all primes have the same ramification degree. Otherwise we minimise the number of pseudo generators which are input to the normal form computation (of polynomial complexity in the degree of the field). For a discussion of improvements to and the complexity of the Hermite normal form computation see [**BFH14**]. The generic procedure to compute a basis from generators which uses a normal form computation is not often required as we mostly directly compute a basis in a normal form. Our computation of maximal orders also does not require the computation of any intermediate P-maximal orders as in some other algorithms.

In this chapter we provide the common background information for the computation of maximal orders in the 3 different types of cyclic extensions. We provide a comparison of timings in Sections 2.7, 3.7 and 5.8. We use several results presented in [**Sti93**] and [**Fra05**] and also follow some notation used in this book (especially Chapter I and III) and thesis.

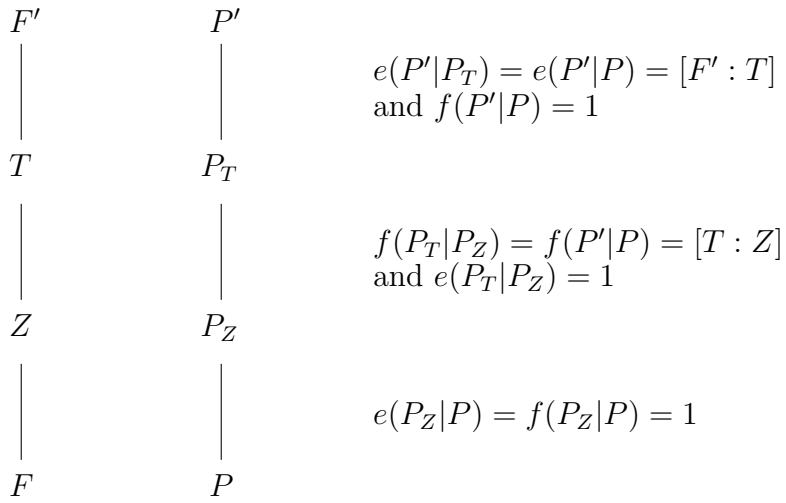
1.1. Ramification Theory in Galois Extensions

Since we are working with Galois extensions of function fields we have, from Hilbert's ramification theory, that $e(P_i|P) = e(P_j|P)$ for ideals $P_i, P_j \mid P$ and similarly $f(P_i|P) = f(P_j|P)$. We also have $e(P'|P)f(P'|P)r = [F' : F]$ where r is the number of places of F' which extend P.

Let $G = \mathrm{Gal}(F'/F)$ be the Galois group of F'/F. We also have the *decomposition group* $G_Z(P'|P) = \{\sigma \in G | \sigma(P') = P'\}$ and the *inertia group* $G_T(P'|P) = \{\sigma \in G | v_{P'}(\sigma(z) - z) > 0 \forall z \in \mathcal{O}_{P'}\}$ of $P' \mid P$, which satisfy $G_T(P'|P) \subseteq G_Z(P'|P) \subseteq G$. The fixed fields of these groups are called the *decomposition field* and *inertia field* respectively.

Theorem 1.1 ([**Sti93**] Theorem III.8.2 (d))**.** *Let F'/F be a Galois extension, P a place of F and P' an extension of P to F'. Let P_Z and P_T denote the restriction of P' to the*

decomposition field Z and inertia field T respectively of $P' \mid P$. Then we have the following picture



So P is completely decomposed or split in Z/F, P_Z is completely inert in T/Z and P_T is totally ramified in F'/T.

1.2. Class Field Theory

It is possible to count the number of rational places in abelian extensions ([**Coh00**] Theorem 3.5.3) hence class field theory is a powerful technique for constructing extensions with many rational places.

As abelian groups can be decomposed into a finite product of cyclic groups so can abelian extensions be decomposed into cyclic extensions of prime power degree ([**DF12**] Section 3.1). We call these cyclic extensions the *components* of an abelian extension. The integral closure in an abelian extension can be computed from the integral closures in the cyclic component extensions hence computing integral closures efficiently in cyclic extensions can improve the efficiency of the computation of integral closures in abelian extensions. The improvement to the efficiency of the construction of good large codes can be seen most notably when constructing codes from cyclic extensions. Note that in some cases, such as Hilbert class fields where the discriminants of the integral closures of the components are 1, our combination of the integral closures of the components is an integral closure in the abelian extension, however in the general case, another integral closure algorithm will need to be applied to finish the computation in the abelian extension. This may be considerably more expensive than the computations in the component extensions.

1.3. Integral Closures

Let F'/F be a finite separable extension of the global algebraic function field F/K, and $P \in \mathbb{P}_F$ be a place of F/K. Recall from [**Sti93**] Corollary III.3.5 that the integral closure $\mathcal{O}'_P$ of the valuation ring $\mathcal{O}_P = \{z \in F | z^{-1} \notin P\}$ in F' is

$$\mathcal{O}'_P = \bigcap_{P'|P} \mathcal{O}_{P'}$$

where $\mathcal{O}_{P'}$ is the valuation ring at the place $P' \mid P$. We also have from this corollary that there is a basis $\{a_i\}_{0 \leq i < n}, n = \deg(F'/F)$ of F'/F such that

$$\mathcal{O}'_P = \sum_{i=1}^{n} \mathcal{O}_P a_i$$

and we call such a basis $\{a_i\}_{0 \leq i < n}$ an *integral basis* of $\mathcal{O}'_P$ over $\mathcal{O}_P$ or a *P-integral basis*.

Therefore we have that $\mathcal{O}'_P$ contains those elements of F' with non-negative valuation at all primes $P' \mid P$.

For sets $S \subset \mathbb{P}_F$, we have *holomorphy rings* $\mathcal{O}_S = \cap_{P \in S} \mathcal{O}_P$. As noted by [**Fra05**] following Proposition 1.2.8, the integral closure of $\mathcal{O}_S$ in F'/F is

$$\mathcal{O}'_S = \bigcap_{P'|P, P \in S} \mathcal{O}_{P'} = \bigcap_{P \in S} \mathcal{O}'_P.$$

We also note from [**Fra05**] Proposition 1.2.8 (iii) that $\mathcal{O}_S$ is a Dedekind domain and from [**Sti93**] Proposition III.2.9 that there is a 1-1 correspondence between S and the set of maximal ideals of $\mathcal{O}_S$ given by

$$P \longleftrightarrow \mathcal{O}_S \cap P.$$

We consider some special cases of holomorphy rings corresponding to S being the finite places, $\mathbb{P}_F^0$, and infinite places, $\mathbb{P}_F^\infty$. These holomorphy rings are the *finite* and *infinite maximal orders*, $\mathbb{Z}_F^0$ and $\mathbb{Z}_F^\infty$, as mentioned in the Background and Notation and [**Fra05**] following Remark 1.2.9 and as computed by Magma [**CBFS13**]. Note that since $\mathbb{P}_F^\infty$ is a finite set, $\mathbb{Z}_F^\infty$ is a principal ideal domain ([**Sti93**] Proposition III.2.10) but $\mathbb{Z}_F^0$ is not always. We do not use the principal ideal domain property. We denote a maximal order or "ring of integers" of a field F by $\mathbb{Z}_F$ when the maximal order could be either finite or infinite. A maximal order $\mathbb{Z}_{F'}$ is equivalent to a holomorphy ring $\mathcal{O}'_S$ where $S = \mathbb{P}_F^0$ or $\mathbb{P}_F^\infty$ because it contains all elements integral over $\mathcal{O}_S = \mathbb{Z}_F$. We have from the correspondence above that the prime ideals of $\mathbb{Z}_F$ correspond to a place P of F, where the finite places of F correspond to an ideal of the finite maximal order and the infinite places of F correspond

to an ideal of the infinite maximal order. We will use P for both the place P and its intersection with the relevant maximal order and refer to the intersection of a place with a maximal order as a *prime* of the maximal order.

1.4. Orders

As [**Sti93**] mentions, holomorphy rings are only one type of subring of a function field. He also mentions subrings of the form $k[t][x_1, \ldots, x_n]$ where $x_1, \ldots, x_n \in F' \setminus k(t)$. We now consider a type of subring of this second form.

An *order* $\mathcal{O}$ of an algebraic function field extension $F'/k(t)$ is a subring of F' containing 1 which has the structure of a finitely generated $k[t]$- or V_∞-module of maximal rank $\deg(F'/k(t))$ over $k[t]$ or V_∞. As [**Coh00**] notes in his introduction, it is common for algebraic fields F'/F to be represented as a finite extension of another algebraic field $F/k(t)$. An order $\mathcal{O}$ of a function field $F'/F/k(t)$ in this *relative representation* is not only a $k[t]$- or V_∞-module but also has the structure of a finitely generated $\mathcal{C}$-module where $\mathcal{C}$ is an order of F. We call $\mathcal{C}$ the *coefficient ring* of $\mathcal{O}$. An order $\mathcal{O} \subset F'$ is contained in the integral closure $\mathbb{Z}_{F'}$ of either $k[t]$ or V_∞ in F'. We consider the rings $k[t]$ and V_∞ to be the orders of the rational function field $k(t)$. An order, as a module over its coefficient ring, has a basis or a pseudo basis in the same way as a function field has a basis as a vector space over its coefficient field. Some orders can be defined by a defining polynomial f such that $\mathcal{O} = \mathcal{C}[x]/f(x)$ or $\mathcal{O} = \mathcal{C}[\alpha]$ where α is a root of a monic polynomial f over $\mathcal{C}$. Such orders are sometimes referred to as *equation orders* and will have $\{\alpha^i\}_{0 \le i < [\mathcal{O}:\mathcal{C}]}$ as a basis. We call such bases consisting of powers of a primitive element a *power basis*. An order $\mathcal{O}$ of an algebraic field extension F'/F is *maximal* over its coefficient ring if it is not contained in any larger order of F'/F over that coefficient ring. A maximal order $\mathcal{O} \subset F'/F$ is equal to the integral closure of its coefficient ring in F'. A maximal order has an *integral basis* or integral pseudo basis, a basis consisting of integral (pseudo) elements over the coefficient ring or equivalently elements integral at all prime ideals contained in the maximal order. An *integral module* is a module contained in an integral closure of its coefficient ring, that is, an integral module contains only elements integral at all finite or infinite places.

The *discriminant* of an order $\mathcal{C}[\alpha]$ is equal to the discriminant of the minimal polynomial of α, the defining polynomial of the extension. The discriminant of a maximal order is equal to the norm of the *different* which is the product $\prod_{P \in \mathbb{P}} \prod_{P'|P} P'^{d(P'|P)}, \mathbb{P} = \mathbb{P}_F^0$ or $\mathbb{P}_F^\infty$, where $d(P'|P)$ is the different exponent of $P' \mid P$ corresponding to the different divisor defined in [**Sti93**] Definition III.4.3. When $P' \mid P$ is unramified $d(P'|P) = 0$,

otherwise in the cases we are considering, $d(P'|P) = e(P'|P) - 1$ in a Kummer extension and $d(P'|P) \geq e(P'|P) - 1$ in an Artin–Schreier extension and the exact value is given in Remark 3.7.

A *Dedekind domain* is a Noetherian, integrally closed domain such that every non-zero prime ideal is a maximal ideal ([**Coh00**] Definition 1.2.1). Most linear algebra algorithms for $\mathbb{Z}$ and $k[t]$-modules can be generalized to modules over Dedekind domains ([**Coh00**] Chapter 1). In particular we can compute a normal form of a module over a Dedekind domain ([**Coh00**] Algorithm 1.4.7) although this can be expensive. To take advantage of this the orders we are interested in will be extensions of a maximal order $\mathbb{Z}_F$ of the function field F since only maximal orders are Dedekind domains, therefore $\mathcal{C}$ will be a maximal order in our discussion. We attempt to construct bases which are already in a normal form.

1.4.1. Pseudo Bases. The algorithms in this part of the thesis compute pseudo bases for maximal orders to describe the maximal order as a module over a Dedekind domain. Analogous to [**Poh96**] we have that a relative integral basis does not exist in every relative extension. A relative integral basis for an order $\mathcal{O} \supseteq \mathcal{C}[\alpha]$ with coefficient ring $\mathcal{C}$ only exists when the quotient of the discriminant of $\mathcal{C}[\alpha]$ by the discriminant of $\mathcal{O}$ is a principal ideal [**Art65**]. If a relative integral basis of $\mathcal{O}$ exists over $\mathcal{C}$ then $\mathcal{O}$ is a free module over $\mathcal{C}$ and its discriminant is a principal ideal of $\mathcal{C}$. The infinite maximal order $\mathbb{Z}_{F'}^{\infty}$ is always a free module since its coefficient ring $\mathbb{Z}_F^{\infty}$ is a principal ideal domain but we have not found it constructive to use this property.

In order to preserve the rich structure of $\mathcal{O}$ as a $\mathbb{Z}_F$-module we need to be able to represent $\mathcal{O}$ as a $\mathbb{Z}_F$-module even though $\mathcal{O}$ is not a free $\mathbb{Z}_F$-module. The theory of $\mathbb{Z}$-bases can be generalized to other euclidean domains and conditionally to principal ideal domains, however, $\mathbb{Z}_F$ is not always a principal ideal domain. Chapter 1 of [**Coh00**] covers the generalization of linear algebra algorithms for $\mathbb{Z}$-modules to $\mathbb{Z}_F$-modules in the case of algebraic number fields, the case of algebraic function fields is analogous.

Since an order is a finitely generated $k[t]$- or V_∞-module it is a finitely generated $\mathbb{Z}_F$-module. Also, an order is torsion free because it contains no zero divisors, therefore by [**Coh00**] Theorem 1.2.18 an order is a projective $\mathbb{Z}_F$-module. Applying [**Coh00**] Corollary 1.2.24 we have for an order $\mathcal{O}$ of degree n with coefficient ring $\mathbb{Z}_F$ there are elements $\omega_1, \ldots, \omega_n \in \mathcal{O}$ and fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_n \subset \mathbb{Z}_F$ such that

$$\mathcal{O} = \mathfrak{a}_1\omega_1 \oplus \cdots \oplus \mathfrak{a}_n\omega_n.$$

We can use this description of $\mathcal{O}$ instead of a basis. To formalize we give Cohen's [**Coh00**] Definition 1.4.1 of pseudo elements and bases and Hoppe's [**Hop98**] Definition 4.1.1 of a pseudo matrix.

Definition 1.2 ([**Coh00**], Definition 1.4.1)**.** *Let M be a finitely generated torsion-free R-module, where R is a Dedekind domain and F is its field of fractions, and let V be an F-vector space such that M is a submodule of V and $V = FM$.*

1. *A pseudo-element of V is a sub-R-module of V of the form $\mathfrak{a}\omega$ with $\omega \in V$ and $\mathfrak{a}$ a fractional ideal of R, or equivalently an equivalence class of pairs $(\omega, \mathfrak{a})$ formed by an element of V and a fractional ideal of R under the equivalence relation $(\omega, \mathfrak{a}) \sim (\omega', \mathfrak{a}')$ if and only if $\mathfrak{a}\omega = \mathfrak{a}'\omega'$ as sub-R-modules of rank 1 of V.*
2. *The pseudo-element $\mathfrak{a}\omega$ is said to be integral if $\mathfrak{a}\omega \subset M$.*
3. *If $\mathfrak{a}_i$ are fractional ideals of R and ω_i are elements of V, we say that $(\omega_i, \mathfrak{a}_i)_{1 \leq i \leq m}$ is a pseudo-generating set for M if*
$$M = \mathfrak{a}_1\omega_1 + \cdots + \mathfrak{a}_m\omega_m.$$
4. *We say that $(\omega_i, \mathfrak{a}_i)_{1 \leq i \leq m}$ is a pseudo-basis of M if*
$$M = \mathfrak{a}_1\omega_1 \oplus \cdots \oplus \mathfrak{a}_m\omega_m.$$

From a pseudo-generating set or basis we can construct a pseudo matrix by putting the vectors w_i into the columns (or rows) of a matrix.

Definition 1.3 ([**Hop98**], Definition 4.1.1)**.** *Let $\mathcal{O}$ be an order of a field F and let $m, n \in \mathbb{N}$ and A be an $(n \times m)$-matrix over F with column vectors $A_1, \ldots A_m$ in F^n. Let $\mathfrak{a}_1, \ldots \mathfrak{a}_m$ be fractional ideals of $\mathcal{O}$. Then the pair $[(\mathfrak{a}_1, \ldots, \mathfrak{a}_m), A]$ is a* pseudo matrix *over $\mathcal{O}$ with n rows and m columns.*

A pseudo matrix constructed from a pseudo basis for an order $\mathcal{O}$ in a field F'/F of degree n will have n rows and n columns. We can use a pseudo matrix $[(\mathfrak{a}_j)_j, A]$ with invertible matrix A as a transformation expressing elements of an order $\mathcal{R} \subset F', \mathcal{R} \subseteq \mathcal{O}$ or $\mathcal{O} \subseteq \mathcal{R}$, as a linear combination of the basis of $\mathcal{O}$ as follows. Let $(r_j, \mathfrak{r}_j)_j$ be a pseudo basis of $\mathcal{R} \subset F'$ and $[(\mathfrak{a}_j)_j, A]$ be a pseudo matrix. Let $\mathcal{O} \subset F'$ be the order with basis $(r_j, \mathfrak{r}_j)_j$ transformed by $[(\mathfrak{a}_j)_j, A]$. Let $r = \sum_j c_j r_j \in \mathcal{R}$, then $\sum_j A_{ji} c_j$ is the ith coefficient of r with respect to the transformed basis of $\mathcal{O}$. Let $(w_j, \mathfrak{a}_j)$ be a pseudo basis of $\mathcal{O}$, then $w_j = \sum_i (A^{-1})_{ji} r_i$. An element $\beta \in F'$ lies in $\mathcal{O}$ if, for all j, the coefficient of the jth basis element of $\mathcal{O}$ in β lies in $\mathfrak{a}_j$.

The *determinant of a module* is the product of the determinant of the matrix A of the pseudo matrix of a pseudo basis for the module and the product of the *coefficient ideals* $\mathfrak{a}_i$ of that pseudo basis.

It is useful to be able to express a pseudo basis in a unique normal form. One such normal form which can be used is the Hermite normal form, a generalization of the extended Euclidean algorithm, [**Coh00**] Theorem 1.4.6. Since we are considering only modules of full rank we can describe the normal form which we use more simply. A pseudo matrix $[(\mathfrak{a}_i), A]$ is in *normal form* if A is a lower (since we use the column vectors of A) triangular matrix with only 1s on its diagonal. The construction of orders from this normal form is more efficient than from an arbitrary basis. There is a different normal form for matrices over polynomials, the Popov form, but we have not used it.

1.4.2. More about Orders. In general, the *discriminant* of an order $\mathcal{O}$ is equal to the product of the determinant of the trace matrix, $\mathrm{Tr}(\omega_i\omega_j)$, of $\mathcal{O}$ with the product of the coefficient ideals $\mathfrak{a}_i$ squared. An order may be constructed by a basis transformation, given by a pseudo matrix, of another order. If an order $\mathcal{R}$ contains an order $\mathcal{O}$ it is a transformation of we call $\mathcal{O}$ a *suborder* of $\mathcal{R}$. The *index* $[\mathcal{R} : \mathcal{O}]$ is the quotient of the determinant of the module $\mathcal{O}$ by the determinant of the module $\mathcal{R}$ which is equal to the square root of the quotient of the discriminant of $\mathcal{O}$ by the discriminant of $\mathcal{R}$. Maximal orders can be constructed by a chain of transformations

$$\mathbb{Z}_F[\alpha] = \mathcal{O}_0 \subset \ldots \subset \mathcal{O}_i \subset \ldots \subset \mathcal{O}_j \subset \ldots \subset \mathbb{Z}_{F'}$$

where $\mathrm{disc}(\mathcal{O}_j) | \mathrm{disc}(\mathcal{O}_i)$ when $i \leq j$ however we construct S-maximal orders as direct transformations of $\mathbb{Z}_F[\alpha]$.

As orders are modules they can be added. The module sum of two orders is equivalent to the smallest order containing both orders when the indices of the orders in a common suborder are coprime. The module addition can be computed by a normal form of the concatenation of the pseudo bases of the module addends ([**Coh00**] Section 1.5.2).

We extend the definition of P-maximal orders to

Definition 1.4. *Let F'/F be a field extension, let S be set of primes of $\mathbb{Z}_F$, the integral closure of $k[t]$ or V_∞ in F and let $\mathbb{Z}_{F'}$ be the integral closure of $\mathbb{Z}_F$ in F'. A module $\mathcal{R} \subseteq \mathbb{Z}_{F'}$ with coefficient ring $\mathbb{Z}_F$ is* S-maximal *if the localizations $(\mathbb{Z}_{F'})_P$ and $\mathcal{R}_P$ are equal for all primes $P \in S$.*

Let $\mathcal{O}$ be an order in the field F'/F with coefficient ring $\mathbb{Z}_F$. The S-maximal over order of $\mathcal{O}$ *is the order $\mathcal{R}$ which is S-maximal and such that $\mathcal{O}$ is a submodule of $\mathcal{R}$ and the localizations $\mathcal{R}_Q$ and $\mathcal{O}_Q$ are equal for primes Q of $\mathbb{Z}_F, Q \notin S$.*

This is equivalent to $\mathcal{R} = \{x \in \mathbb{Z}_{F'} \mid \exists m : (\prod_{P\in S} P)^m x \subset \mathcal{O}\}$ and we also have $[\mathcal{R} : \mathcal{O}] \mid (\prod_{P\in S} P)^m \ \exists m$ and $\gcd([\mathbb{Z}_{F'} : \mathcal{R}], S) = 1$ [**Fie13b**].

Note that [**Coh00**] gives a definition of an order being P-maximal (Definition 2.4.1(1)). His definition concentrates on the difference between a P-maximal order and a maximal order and does not have any reference to a suborder, similar to the first paragraph of our definition. The suborder is important to us as we wish to compute the minimal such S-maximal order when possible. However, since it is advantageous to compute S-maximal modules which are not the minimal S-maximal order in the Artin–Schreier–Witt case we have split the definition above to allow for this.

We mostly allow that $S \subset \mathbb{P}_F$ may be an infinite set, however, we note that there will only be finitely many primes in S which will be of interest. That is, there will be only finitely many primes P for which the Artin–Schreier quotient (Definition 3.2) is non-zero or more generally there are only finitely many primes P such that $v_P(u) \neq 0$ for $u \in F$. This corresponds to there being only finitely many primes P such that an order $\mathcal{O}$ is not already P-maximal.

The pseudo bases we present in this thesis are for S-maximal orders as transformations of equation orders $\mathbb{Z}_F[\alpha]$ having a power basis. In order to construct an S-maximal over order of an order $\mathcal{O}$ which does not have a power basis we compute the smallest order containing $\mathcal{O}$ and the S-maximal order of the equation order $\mathbb{Z}_F[\alpha]$ of $\mathcal{O}$, by module addition if the indices of the S-maximal order of $\mathbb{Z}_F[\alpha]$ and $\mathcal{O}$ in $\mathbb{Z}_F[\alpha]$ are coprime.

1.5. Witt Vectors

We state here the information about Witt vectors which is necessary for Chapter 5. For a more thorough treatment see [**Fra05**] Section 1.4 and [**Wit36, Has80**, p. 156–161].

Definition 1.5. *Let R be a commutative ring and let $n > 0$. The ring $W_n(R)$ of Witt vectors of length n is the set of all vectors of length n with entries in R with addition and multiplication given by that of the secondary components below and zero $(0, \ldots, 0)$ and one $(1, 0, \ldots, 0)$.*

A Witt vector $x = (x_1, \ldots, x_n)$ is completely determined by its secondary components

$$x^{(i)} = \sum_{j=1}^{i} p^{j-1} x_j^{p^{i-j}}$$

for which we have the formulas

$$x^{(1)} = x_1, \qquad x^{(i)} = (x^p)^{(i-1)} + p^{i-1} x_i$$

where $x^p = (x_1^p, x_2^p, \ldots, x_n^p)$. We also have $(x \pm y)^{(i)} = x^{(i)} \pm y^{(i)}$ and $(x \times y)^{(i)} = x^{(i)} \times y^{(i)}$. We use addition and subtraction in the computation of Artin–Schreier–Witt quotients so we give a direct formula also here.

Proposition 1.6 ([**Fra05**], Proposition 1.4.2)**.** *Let A, B be Witt vectors in $W_n(R)$ where R has characteristic 0. Then*

$$(A \pm B)_i = A_i \pm B_i + \frac{A_{i-1}^p \pm B_{i-1}^p - (A \pm B)_{i-1}^p}{p} + \frac{A_{i-2}^{p^2} \pm B_{i-2}^{p^2} - (A \pm B)_{i-2}^{p^2}}{p^2} + \ldots \ldots + \frac{A_1^{p^{i-1}} \pm B_1^{p^{i-1}} - (A \pm B)_1^{p^{i-1}}}{p^{i-1}}$$

Let $X = (X_1, \ldots, X_n)$ and $Y = (Y_1, \ldots, Y_n)$ where $X_1, \ldots, X_n, Y_1, \ldots, Y_n$ are indeterminates of a polynomial ring over $\mathbb{Z}$ with rank $2n$. When $A, B \in W_n(R)$ where R has characteristic $p > 0$, $(A \pm B)_i = (X \pm Y)_i(A_1, \ldots, A_n, B_1, \ldots, B_n)$, that is, $A \pm B$ is the evaluation of $X \pm Y$ at the concatenation of the entries of A and B.

1.6. Complexity

We introduce here the notation we use for asymptotic formulas to describe the complexity or running times of our algorithms. These formulas describe the rate of growth of the running time compared to some size of the input to the algorithm, we will use mostly the degree of the field extension. For detailed explanations please see [**CLR90, Knu97**]. We compute complexity by counting operations in a coefficient ring.

We say that an algorithm has complexity $O(h(n))$ when a function $g(n)$ describing its running time is in

$$O(h(n)) = \{g(n) : \exists c > 0 \text{ and } n_0 \text{ such that } 0 \leq g(n) \leq ch(n)\ \forall n \geq n_0\}.$$

The notation $O(h(n))$ describes an asymptotic upper bound and is used for worst case complexity, the most commonly stated.

When $h(n)$ is polynomial in n we say that the algorithm has (at best or worst) polynomial complexity in n. We can also describe the complexity of an algorithm as linear, quadratic, exponential or logarithmic if $h(n)$ is any of these.

Let n be the degree of the function field extension F'/F defined by the polynomial $f(x)$. Addition and subtraction of elements of F' incurs a cost of n additions or subtractions in F so we say these operations have complexity $O(n)$. Multiplication of elements of F' with respect to an arbitrary basis may incur n^3 multiplications in F which would imply a complexity of $O(n^3)$ however, for elements of equation orders and fields, which can be represented as polynomials in some primitive element, multiplication and division (which can be computed using a recursive algorithm that maps the computation to a multiplication) can be computed in $n\log(n)\log(\log(n))$ operations in F using the Fast Fourier Transform based Schönhage-Straßen [**SS71**] algorithm for multiplication of polynomials. Division of polynomials can also be done using linear algebra having complexity $O(n^3)$. The inclusion of division here covers the reduction of elements modulo the defining polynomial of the extension so that we can say that the complexity of multiplication of elements with respect to a power basis is in $O(n\log(n)\log(\log(n)))$. The mth powers of an element in F' can be computed in $\log_2(m)$ multiplications in F' so powering of elements in F' uses $O(\log(m)n\log(n)\log(\log(n)))$ operations in F.

In [**BFH14**] a modular algorithm for computing a Hermite normal form of a full rank n square module over a Dedekind domain is presented. It is polynomial complexity in n ($O(n^3)$) and the degree d ($O(d^7)$) of the Dedekind domain over the integers of the rational (function) field. For the rectangular case the complexity is $O(n^2m)$ where m is the number of pseudo generators.

There are several different ways in which ideals can be multiplied which depend on whether the ideal is represented by 2 generating elements or by a basis. At worst the product of ideals in a degree n extension requires n matrix multiplications of $n\times n$ matrices, a $O(n^3)$ operation, followed by a normal form computation on a $n^2\times n$ matrix. At best it requires 2 element multiplications but more likely 4 element multiplications and a normal form computation on a $4n\times n$ matrix, an $O(n^3)$ operation. Therefore the complexity of ideal multiplication is at worst $O(n^4)$. Taking the mth power of an ideal requires $\log_2(m)$ ideal multiplications. Computing valuations $v_P(u)$ of elements $u\in F$ at ideals $P\subset F$

by [**Ber05**] Algorithm E requires $3\log_2(v_P(u))$ element operations in F so we state the complexity of this computation as $O(\log_2(v_P(u)))$.

Strong approximation does divisor operations then loops over the primes doing a Riemann Roch space calculation ([**Heß99**]) for some divisor related to the prime. For each basis element of the Riemann Roch space it writes it as a series expansion to some precision of a sum of powers of some uniformizing element then solves a system of linear equations over a finite field. Chinese remainder loops over number of primes doing polynomial time extended euclidean ([**Coh00**] Proposition 1.3.1).

Addition of Witt vectors in $W_n(R)$ using the formulas in Proposition 1.6 involves the computation of n entries, and for the computation of the ith entry a sum of at least i terms each involving 3 powers and 3 additions needs to be evaluated. Therefore addition of Witt vectors involves

$$\begin{aligned}\sum_{i=1}^{n} i(\log(p^{i-1})n\log(n)\log(\log(n))) &= \log(p)n\log(n)\log(\log(n))\sum_{i=1}^{n} i(i-1)\\ &= \log(p)n\log(n)\log(\log(n))(\sum_{i=1}^{n} i^2 - \sum_{i=1}^{n} i)\\ &= \log(p)n\log(n)\log(\log(n))(n/2\ O(n^2) - n(n+1)/2)\\ &= O(\log(p)n^4\log(n)\log(\log(n))\end{aligned}$$

operations in F.

1.7. Previous Work

Maximal orders in finite extensions of number fields and function fields can be computed using the Round 2 [**Coh00**] or Round 4 [**Bai96, FL94**] algorithms which both have polynomial complexity in the degree of the field. To compute a maximal order using these algorithms we factor the discriminant of the input order and compute P-maximal orders for every prime P dividing this discriminant. Note that the computation of a maximal order in a number field is usually polynomial time equivalent to finding the squarefree factorization of the discriminant and the computation of a maximal order in a global function field is usually polynomial time in the degree and the logarithm of the characteristic [**Chi89**]. However, we do not require a full factorization of discriminants for most of our maximal order computations. While we do need to know the primes the orders are not yet maximal at, these can be computed from the GCD of a discriminant polynomial and its derivative when the extension is of the rational function field (any primes the order is not maximal at

occur in the discriminant). We do not require the potentially more expensive computation of their valuation in the discriminant, an $O(\log_2(v_P(\text{disc})))$ computation. In fact, most of the primes of interest can be found in the constant coefficient of the defining polynomial, or in the Artin–Schreier–Witt case the Witt vector which describes the constant coefficients of the polynomials defining the relative representation of the function field. Both of these are usually smaller than the discriminant and so cheaper to extract primes from.

The P-maximal orders once computed by Round 2 are added as modules to obtain the maximal order itself. While we first approached maximal order computations by computing P-maximal orders more efficiently and adding them we discovered we could gain more than this. We compute S-maximal orders, including maximal orders, of cyclic extensions without computing P-maximal orders as an intermediate step. We can do this because we construct a pseudo basis for an S-maximal order (Proposition 2.4, Theorem 3.8, Theorem 5.9) and not only for a P-maximal order.

[**Pau01**] provides an algorithm for factoring polynomials over local fields. The factorizations computed by this algorithm are certified by two element certificates which can be used to compute a P-maximal order of an equation order where the polynomial is factored over the completion of its coefficient ring at P.

The Montes Algorithm ([**GMN11, GMN12, GMN13**]) has been used in [**Bau14**] to compute integral bases for fractional ideals in function fields. This is achieved by factorizing the defining polynomial of an extension $F/k(t)$ over the completion of $k(t)$ at each prime polynomial $P(t)$ which is a factor of the discriminant of the defining polynomial of $F/k(t)$ with the Montes algorithm and using the information this algorithm computes to compute $P(t)$-integral bases which are then merged into an integral basis for the input ideal $I \subset F'$. This is a similar approach to [**Pau01**] however it uses a different factorization technique which is faster.

Previous algorithms to compute maximal orders in specific types of cyclic extensions have involved computing an order generated from a list of elements.

1.7.1. Kummer Extensions. Earlier work on computing maximal orders of radical extensions has concentrated on computations in Kummer extensions (Definition 2.1).

Let P be a prime in an algebraic field F . Generators of P-maximal orders of Kummer extensions of F are well known (for number fields [**Dab95, Poh96, Dab01**], for function fields [**Fra05**]). However, it is expensive to construct a P-maximal order from those generators as the generic procedure to compute a basis from these generators is at least an $O(n^3)$ computation, where n is the degree of the field, because of the use of normal forms.

In the publications [**Dab95, Poh96, Dab01**] a system of generators for the maximal order of a Kummer extension ([**Dab95**] Theorem 3.29 and [**Poh96**] Theorem 2.3) is provided. They restrict to Kummer extensions of prime degree and reduction of generators is required. After reduction they have at most twice the degree number of generators. They are also interested in relative discriminants (of maximal orders) of Kummer extensions.

Fraatz [**Fra05**] also computes generators for maximal orders of Kummer extensions of function fields. There is no theoretical restriction on the degree of the extension and the number of generators is related to the number of ramified primes. We will compare timings using our implementation of our algorithms with his implementation of his algorithm as well as the Magma implementation of Round 2 in Section 2.7 where we notice that [**Fra05**] is a substantial improvement on Round 2 and our implementation is a substantial improvement on his.

Cohen [**Coh00**] states Hecke's Theorem. In his proof of Hecke's Theorem (Theorem 10.2.9) he gives elements which are Kummer equivalent (Definition 10.2.8) to the constant coefficient of the defining polynomial of the Kummer extension but such that a root of this Kummer equivalent element will generate a P-integral power basis of the Kummer extension ([**Sti93**] Propositions III.5.11 and 12) when P is either totally ramified or unramified in the extension. We use such a root of a Kummer equivalent element to form a P-integral power basis in Theorem 2.2. At the end of his Subsection 5.3.6 he claims that computing an integral pseudo basis of a Kummer extension is easy but he does not give an algorithm. We do provide an algorithm and shall show that it indeed is a very efficient computation.

Stichtenoth [**Sti93**] states and proves the values of the ramification degrees and different exponents of primes of a Kummer extension of F over P in Proposition III.7.3 and its proof. Elements generating a P-integral power basis of a Kummer extension can be deduced from this proof.

1.7.2. Artin-Schreier–Witt Extensions. Fraatz [**Fra05**] has been the first to investigate Artin-Schreier–Witt extensions algorithmically. He considers the computation of maximal orders of these extensions. However, like previous computations of maximal orders of Kummer extensions mentioned above this approach also computes the maximal order by writing down a generating set and obtaining a basis from this by a generic procedure which is at least an $O(n^3)$ computation, where n is the degree of the field extension, because of the use of a normal form computation [**Coh00**] (Algorithm 1.4.7 and Remark following). We compare times using our implementation to that of [**Fra05**] in Sections 3.7

and 5.8 where we again notice that his implementation is a substantial improvement on Round 2 and our implementation is a substantial improvement on his.

Chapter 2

Kummer Extensions

Definition 2.1 ([**Sti93**] III.7.3)**.** *Let F be a algebraic field containing a primitive n-th root of unity, where $n > 1$ is coprime to the characteristic of F, and let $u \in F$ be such that $u \neq w^d$ for all $w \in F$ and $d > 1, d \mid n$. Then $F' = F(\alpha)$ with $\alpha^n = u$ is a Kummer extension of F.*

A Kummer extension of degree n is a cyclic Galois extension whose automorphisms are described by $\beta \mapsto \zeta\beta$ where ζ is an n-th root of unity in F.

Although we focus on Kummer extensions in this chapter we note that the algorithms described in this chapter are applicable to the more general case of *radical* extensions for which we do not require that F contain a primitive n-th root of unity. Some results may be stated for radical extensions however it is in the case of Kummer extensions we anticipate that our efficient algorithm will be the most used.

Even more generally, in this chapter, our results also hold when F is a number field. The results in this chapter also appear in [**Sut12**].

2.1. A P-integral Power Basis

For a Kummer extension $F' = F(\alpha)$ Stichtenoth [**Sti93**] (Theorem III.7.3 and its proof) suggests an isomorphic Kummer extension $E = F(\beta)$ such that β defines a P-integral power basis for F'. The suggested β is such that $\beta = \alpha^l\gamma^j$ for some $\gamma \in F$ and some l coprime to n, that is, β^n is Kummer equivalent to α^n, ([**Coh00**] Definition 10.2.8). Note that Stichtenoth does not use the existence of a primitive n-th root of unity in the coefficient field so we state our theorem for radical extensions.

Theorem 2.2 (P-integral power basis of a radical extension)**.** *Let F'/F be a radical extension defined by the polynomial $x^n - u$ and let α be a root of this polynomial, a primitive element for F'. Let P be a place of F with $v_P(n) = 0$. Set g_P, k_P, j_P such that $g_P = k_P v_P(u) + nj_P, 0 \leq g_P < n$ and g_P is minimal (i.e. $g_P = \gcd(v_P(u), n) \mod n$).*

- *If $g_P \leq 1$ then $\{\beta^i\}_{0 \leq i < n}$ is a P-integral power basis for F' where $\beta = \alpha^{k_P}\pi^{j_P}$ and π is a uniformizing element for P.*

- *If $g_P > 1$ then $\{\beta_1^i \beta_2^l\}_{0 \le i < g, 0 \le l < n/g}$ is a P-integral power basis for F' where*

$$\beta_1 = \alpha^{(n/g_P)} \pi^{(-v_P(u)/g_P)}, \beta_2 = \alpha^{k'_P} \pi^{j'_P} \text{ with } \frac{v_P(u)}{g_P} k'_P + \frac{n}{g_P} j' = 1.$$

(That is β_1 is a root of $x^{g_P} - \beta_1^{g_P} = x^{g_P} - u\pi^{(-v_P(u))}$ and β_2 is a root of $x^{(n/g_P)} - (\alpha^{k'_P} \pi^{j'_P})^{(n/g_P)}$)

Proof. For any place P' of $F', P' \mid P$, we know P' has ramification degree n/g_P over P ([**Sti93**]) for $g_P > 0$ and ramification degree 1 for $g_P = 0$.

We consider 3 cases :

1. $P' \mid P$ is totally ramified : $g_P = 1$,

$$v_{P'}(\beta) = k_P v_{P'}(\alpha) + j_P v_{P'}(\pi) = k_P v_{P'}(\alpha) + j_P \frac{n}{g_P} = 1$$

   Therefore β is a P'-prime element so by [**Sti93**] Proposition III.5.12, $\{\beta^i\}_{0 \le i < n}$ is a P-integral basis for F'.

2. $P' \mid P$ is unramified : $g_P = 0, k_P = 1, j_P = -v_P(u)/n$

$$v_{P'}(\beta) = k_P \frac{v_P(u)}{n} + j_P = \frac{v_P(u)}{n} - \frac{v_P(u)}{n} = 0$$

   The minimal polynomial of β is

$$\phi = x^n - \beta^n = x^n - u^{k_P} \pi^{j_P n}$$

   and

$$v_P(u^{k_P} \pi^{j_P n}) = k_P v_P(u) + j_P n v_P(\pi) = 0$$

   so the minimal polynomial ϕ is integral at P and

$$v_{P'}(\phi'(\beta)) = v_{P'}(n\beta^{n-1}) = v_{P'}(n) + (n-1) v_{P'}(\beta) = 0$$

   so that $\{\beta^i\}_{0 \le i < n}$ is a P-integral basis for F' by [**Sti93**] Proposition III.5.11. Note that this does not hold when $v_P(n)$ is not zero, i.e. when P is a critical prime.

3. When $g_P > 1$, $P' \mid P$ is ramified but not totally. We split F' into a tower of extensions and consider $F'/F_0/F$ where $F_0 = F(\alpha_0)$ and $F' = F'_0(\alpha)$ and $\alpha_0 = \alpha^{n/g_P}$. Let $P_0 = P' \cap F'_0$ then $\gcd(g_P, v_P(u)) = g_P \equiv 0 \mod g_P$ so $P_0 \mid P$ is unramified and $\beta_1 = \alpha_0^{k_P} \pi^{j_P}$ with $k_P = 1$ and $j_P = -v_P(u)/g_P$, $v_{P_0}(\beta_1) = 0$ as for case 2 above. Therefore $\{\beta_1^i\}_{0 \le i < g_P}$ is a P-integral basis for F_0/F.

   Consider $P' \mid P_0$. This is totally ramified since

$$\gcd(n/g_P, v_{P_0}(\alpha^{n/g_P})) = \gcd(n/g_P, v_P(\alpha^{n/g_P})) = \gcd(n/g_P, v_P(u)/g_P) = 1.$$

Therefore we have $\beta_2 = \alpha^{k'_P}\pi^{j'_P}$ as in case 1 above with $v_{P'}(\beta_2) = 1$ so $\{\beta_2^l\}_{0\le l<n/g_P}$ is a P-integral power basis for F'/F_0.

We have then that $\{\beta_1^i\beta_2^l\}_{0\le i<g,0\le l<n/g}$ is a basis for F'/F. Since $v_{P'}(\beta_2) = 1$ and $v_{P'}(\beta_1) = (n/g_P)v_{P_0}(\beta_1) = 0$ both β_1 and β_2 are P'-integral and so $\{\beta_1^i\beta_2^l\}$ is a P-integral basis for F'/F.

□

2.2. A Pseudo Basis

We can construct a pseudo basis from the P-integral power basis of Theorem 2.2 in each case above. We will show that the pseudo basis we construct is a pseudo basis for an order and not only a module and that the order with this pseudo basis contains the equation order. We will prove P-maximality later. We first state a proposition for one place and then extend this proposition to one for any finite number of places.

Proposition 2.3. *Suppose we satisfy the hypothesis of Theorem 2.2. Let $\mathbb{Z}_F$ be the integral closure of $k[t]$ or V_∞ in F and let $\mathcal{O} = \mathbb{Z}_F[\alpha]$ be an order of F' and let $P \subset F$ now denote $P \cap \mathbb{Z}_F$.*

- *If P either totally ramifies or is unramified in F'/F then*

$$(\omega_i, \mathfrak{a}_i)_i = (\alpha^{k_{P,i}}, P^{\mu_{P,i}})_{0\le i<n}$$

is a pseudo basis for an order $\mathcal{R}$ containing $\mathcal{O}$, where $\mu_{P,i} = j_P i + v_P(u)t_{P,i}$ and $k_P i = k_{P,i} + t_{P,i}n, 0 \le k_{P,i} < n$.
- *Otherwise*

$$(\omega_{il}, \mathfrak{a}_{il})_i = (\alpha^{k_{P,il}}, P^{\mu_{P,il}})_{0\le i<g_P,0\le l<n/g_P}$$

is a pseudo basis for an order $\mathcal{R}$ containing $\mathcal{O}$, where

$$\mu_{P,il} = -iv_P(u)/g_P + j'_P l + v_P(u)t_{P,il}$$

and $in/g_P + k'_P l = k_{P,il} + t_{P,il}n, 0 \le k_{P,il} < n$.

These pseudo bases are derived from the P-integral power basis as follows. We prove only the generalization, Proposition 2.4.

- When P totally ramifies or is unramified in F'/F, a P-integral basis is

$$\{\beta^i\}_{0\le i<n},\ \beta = \alpha^{k_P}\pi^{j_P},\ k_P v_P(u) + nj_P = g_P,\ g_P = 0, 1.$$

Using pseudo elements,

$$\begin{aligned}(\alpha^{k_P}P^{j_P})^i &= \alpha^{k_{P,i}}\alpha^{t_{P,i}n}P^{j_Pi} && \text{where } k_Pi = k_{P,i} + t_{P,i}n \text{ and } 0 \le k_{P,i} < n\\ &= \alpha^{k_{P,i}}u^{t_{P,i}}P^{j_Pi}\\ &= \alpha^{k_{P,i}}\pi^{v_P(u)t_{P,i}}u'^{t_{P,i}}P^{j_Pi} && \text{where } u = \pi^{v_P(u)}u'\\ & && \text{and } \pi \text{ is a uniformizing element for } P\end{aligned}$$

We group the P parts together and note that multiplication by u' does not change the exponent of P to get the pseudo basis $(\alpha^{k_{P,i}}, P^{\mu_{P,i}})_{0\le i<n}$.

We also note that since k_P is coprime to n ($k_P = 1$ or $g_P = 1$) and $k_{P,i_1} = k_{P,i_2}$ implies that $k_P(i_1 - i_2) = (t_{P,i_1} - t_{P,i_2})n$ we have $k_{P,i_1} = k_{P,i_2}$ implies that $i_1 = i_2$. So the values $k_{P,i}$ are unique and since there are n different $k_{P,i}$ values, for each $0 \le z < n$ there is some i such that $k_{P,i} = z$.

- When P partially ramifies in F'/F, a P-integral basis is

$$\{\beta_1^i\beta_2^l\}_{0\le i<g_P, 0\le l<n/g_P},\ \beta_1 = \alpha^{n/g_P}\pi^{-v_P(u)/g_P},\ \beta_2 = \alpha^{k'_P}\pi^{j'_P}$$

where $(v_P(u)/g_P)k'_P + (n/g_P)j'_P = 1$. Using pseudo elements,

$$\begin{aligned}&(\alpha^{n/g_P}P^{-v_P(u)/g_P})^i(\alpha^{k'_P}P^{j'_P})^l\\ &= \alpha^{k_{P,il}}\alpha^{t_{P,il}n}P^{-iv_P(u)/g_P + j'_Pl}\\ &\qquad\qquad \text{where } in/g_P + k'_Pl = k_{P,il} + t_{P,il}n \text{ and } 0 \le k_{P,il} < n\\ &= \alpha^{k_{P,il}}u'^{t_{P,il}}P^{-iv_P(u)/g_P + j'_Pl + v_P(u)t_{P,il}}\end{aligned}$$

We note that multiplication by u' does not change the exponent of P to get the pseudo basis $(\alpha^{k_{P,il}}, P^{\mu_{P,il}})_{0\le i<g_P, 0\le l<n/g_P}$.

Here again the $k_{P,il}$ are unique. If $k_{P,i_1l_1} = k_{P,i_2l_2}$ then $(l_1 - l_2)k'_P = n/g_P((t_{P,i_1l_1} - t_{P,i_2l_2})g_P - (i_1 - i_2))$ and since k'_P and n/g_P are coprime $n/g_P \mid l_1 - l_2 < n/g_P$ so $l_1 = l_2$. Let $t_m = t_{P,i_ml_m}$. Then we have $g_P(t_1 - t_2) = i_1 - i_2$ so $g_P \mid i_1 - i_2 < g_P$ and $i_1 = i_2$. Therefore, since there are n different $k_{P,il}$ values, for each $0 \le z < n$ there is some i and l such that $k_{P,il} = z$.

We now directly state a pseudo basis for an order given a set of primes S using a rearrangement of the pseudo basis we have derived and combining for $P \in S$.

Proposition 2.4. *Suppose we satisfy the hypothesis of Proposition 2.3. Let $\mathcal{O} = \mathbb{Z}_F[\alpha]$ be an order of F' and S be a set of primes of $\mathbb{Z}_F$. Then*

$$(\omega_i, \mathfrak{a}_i)_{0\le i<n} = (\alpha^i, \prod_{P\in S} P^{\mu_{P,i}})_{0\le i<n}$$

is a pseudo basis for an order $\mathcal{R}$ containing $\mathcal{O}$ where

$$\mu_{P,i} = \begin{cases} j_P i_P + v_P(u)t_{P,i_P}, & \text{if } P \text{ is unramified or totally ramified in } F' \\ & \text{and } i_P \text{ is such that } i = k_{P,i_P}, 0 \le i_P < n \\ -i_P v_P(u)/g_P + j'_P l_P + v_P(u)t_{P,i_P l_P}, & \text{otherwise with } i_P, l_P \text{ such that } i = k_{P,i_P l_P} \\ & 0 \le i_P < g_P, 0 \le l_P < n/g_P \end{cases}$$

Proof. Let $\mathcal{R}$ be the module with pseudo basis $(\omega_i, \mathfrak{a}_i)_i$. We will show that $\mathcal{R}$ is an order in detail assuming the primes in S are either unramified or totally ramified in F' and note that closure under multiplication can be proven similarly when some primes in S may be partially ramified.

When $i = 0, \omega_0 = 1, \mathfrak{a}_0 = 1$ so $1 \in \mathcal{R}$. We now use pseudo elements and check that $\mathfrak{a}_{i_1}\omega_{i_1} \times \mathfrak{a}_{i_2}\omega_{i_2} \subset \mathcal{R}$. For $i_1, i_2 < n$ and $P \in S$ unramified or totally ramified in F' we have $i_{1,P}, i_{2,P} < n$ so $i_{1,P} + i_{2,P} = m_P n + i_{3,P}, i_{3,P} < n, m_P = 0, 1$ and $i_1 + i_2 = i_3 + (t_{P,i_{3,P}} + k_P m_P - (t_{P,i_{1,P}} + t_{P,i_{2,P}}))n$ by definition of $i_{1,P}, i_{2,P}$ and $i_{3,P}$. So

$$\mathfrak{a}_{i_1}\omega_{i_1} \times \mathfrak{a}_{i_2}\omega_{i_2} = \prod_{P\in S} P^{\mu}\alpha^{i_1+i_2} \tag{1}$$

where

$$\mu = \mu_{P,i_1} + \mu_{P,i_2} = j_P(m_P n + i_{3,P}) + v_P(u)(t_{P,i_{1,P}} + t_{P,i_{2,P}})$$

and

$$i_1 + i_2 = i_3 + n(t_{P,i_{3,P}} + k_P m_P - (t_{P,i_{1,P}} + t_{P,i_{2,P}})).$$

Since $\alpha^n = u$ we can move the u factor of $\alpha^{i_1+i_2}$ into the ideals and we consider

$$\begin{aligned} &\mu_{P,i_1} + \mu_{P,i_2} + v_P(u)(t_{P,i_{3,P}} + k_P m_P - (t_{P,i_{1,P}} + t_{P,i_{2,P}})) \\ &= j_P i_{3,P} + j m_P n + v_P(u)(t_{P,i_{1,P}} + t_{P,i_{2,P}}) + v_P(u)(t_{P,i_{3,P}} + k_P m_P - (t_{P,i_{1,P}} + t_{P,i_{2,P}})) \\ &= j_P i_{3,P} + v_P(u)t_{P,i_{3,P}} + j m_P n + v_P(u)k_P m_P \end{aligned}$$

as the exponent of an ideal P in the adjusted product (1) above and multiplied by $\alpha^{k_{i_3}} = \alpha^{i_3}$ we have

$$\begin{aligned}\mathfrak{a}_{i_1}\omega_{i_1} \times \mathfrak{a}_{i_2}\omega_{i_2} &= \mathfrak{a}_{i_3}\omega_{i_3} P^{j_P m_P n + v_P(u) k_P m_P} \\ &\subseteq \mathfrak{a}_{i_3}\omega_{i_3}\end{aligned}$$

since $j_P m_P n + v_P(u) k_P m_P = m_P g \geq 0$ when all $P \in S$ are unramified or totally ramified in F'. Therefore $\mathfrak{a}_{i_1}\omega_{i_1} \times \mathfrak{a}_{i_2}\omega_{i_2} \subset \mathcal{R}$.

To see that $\mathcal{R}$ contains $\mathcal{O}$ it is sufficient to show that $\alpha \in \mathcal{R}$ since $\mathcal{R}$ is an order. We have $\alpha = 1 \times \omega_1$ and if $1 \in \mathfrak{a}_1 = \prod_{P \in S} P^{\mu_{P,1}}$ then $\alpha \in \mathcal{R}$ and $\mathcal{O} \subseteq \mathcal{R}$. We show that $\mu_{P,i} \leq 0 \ \forall \ 0 \leq i < n, P \in S$.

When

$g_P = 0$**:**

$$\mu_{P,i} = j_P i_P + v_P(u) t_{P,i_P} = \frac{-v_P(u)}{n} i_P + v_P(u) t_{P,i_P} = v_P(u)(t_{P,i_P} - \frac{i_P}{n}) \leq 0$$

since $t_{P,i_P} = \lfloor k_P i_P / n \rfloor$ and $k_P = 1$

$g_P = 1$**:**

$$\begin{aligned} k_P v_P(u) + j_P n = 1, \text{ so } i_P k_P v_P(u) + i_P j_P n &= i_P, \\ i_P = i_P k_P v_P(u) - t_{P,i_P} n v_P(u) + i_P j_P n + t_{P,i_P} n v_P(u) & \\ = v_P(u)(k_P i_P - t_{P,i_P} n) + n(j_P i_P + v_P(u) t_{P,i_P}) & \\ = v_P(u) k_{P,i_P} + n(j_P i_P + v_P(u) t_{P,i_P}), & \\ n(j_P i_P + v_P(u) t_{P,i_P}) = i_P - v_P(u) k_{P,i_P} \leq i_P. & \end{aligned}$$

Therefore $\mu_{P,i} = j_P i_P + v_P(u) t_{P,i_P} \leq i_P / n < 1$, so $\mu_{P,i} \leq 0$.

$1 < g_P < n$**:** Let $\mu = -i_P v_P(u)/g_P + j'_P l_P + v_P(u) t_{P,i_P l_P}$, then

$$\begin{aligned} v_{P'}(\alpha^{k_{P,i_P l_P}} P^{\mu}) &= v_{P'}((\alpha^{n/g_P} P^{-v_P(u)/g_P})^{i_P} (\alpha^{k'_P} P^{j'_P})^{l_P}) \\ &= 0 i_P + 1 l_P = l_P \end{aligned}$$

Therefore,

$$l_P = k_{P,i_P l_P} v_{P'}(\alpha) + v_{P'}(P)(j'_P l_P - i_P \frac{v_P(u)}{g_P} + v_P(u) t_{P,i_P l_P})$$

and

$$\begin{aligned}\frac{n}{g_P}(j'_P l_P - i_P\frac{v_P(u)}{g_P} + v_P(u)t_{P,i_P l_P}) &= l_P - k_{P,i_P l_P} v_{P'}(\alpha)\\ &\leq l_P \text{ since } k_{P,i_P l_P} v_{P'}(\alpha) \geq 0\\ j'_P l_P - i_P\frac{v_P(u)}{g_P} + v_P(u)t_{P,i_P l_P} &\leq l_P\frac{g_P}{n}\\ &< 1 \text{ since } 0 \leq l_P < \frac{n}{g_P}.\end{aligned}$$

Therefore $\mu_{P,i} = j'_P l_P - i_P\frac{v_P(u)}{g_P} + v_P(u)t_{P,i_P l_P} \leq 0$ since the LHS is an integer. So we have in all cases that $\mu_{P,i} \leq 0$ for each $P \in S$. Therefore $\mathcal{O} \subseteq \mathcal{R}$. □

2.2.1. Proof of S-maximality.

Theorem 2.5. *The order with pseudo basis given in Proposition 2.4 is the S-maximal over order of $\mathcal{O}$.*

Proof. Let $\mathcal{R}$ be the order of F'/F with pseudo basis

$$(\omega_i, \mathfrak{a}_i)_{0\leq i<n} = (\alpha^i, \prod_{P\in S} P^{\mu_{P,i}})_{0\leq i<n}$$

where

$$\mu_{P,i} = \begin{cases} j_P i_P + v_P(u)t_{P,i_P}, & \text{if } P \text{ is unramified or totally ramified in } F' \\ & \text{and } i_P \text{ is such that } i = k_{P,i_P}, 0 \leq i_P < n \\ -i_P v_P(u)/g_P + j'_P l_P + v_P(u)t_{P,i_P l_P}, & \text{otherwise with } i_P, l_P \text{ such that } i = k_{P,i_P l_P} \\ & 0 \leq i_P < g_P, 0 \leq l_P < n/g_P \end{cases}$$

To prove that $\mathcal{R}$ is the S-maximal over order of $\mathcal{O}$ we need to prove that $\mathcal{R}_Q = \mathcal{O}_Q$ for all primes Q of $\mathbb{Z}_F, Q \notin S$ and $\mathcal{R}_P = (\mathbb{Z}_{F'})_P \forall P \in S$, where $\mathbb{Z}_{F'}$ is the integral closure of $\mathbb{Z}_F$ in F'.

The determinant of the module $\mathcal{R}$ is a product of non-positive powers of $P \in S$ since $\mu_{Pi} \leq 0$ and the determinant of the identity matrix, whose entries are the coefficients of α^i with respect to the basis of $\mathcal{O}$, is 1 so the determinant has valuation 0 at primes of $\mathbb{Z}_F$ which are not in S. Therefore $\mathcal{R}_Q = \mathcal{O}_Q$ for primes $Q \subset \mathbb{Z}_F, Q \notin S$.

Let $P \in S$. We prove that the elements from our P-integral power basis in Theorem 2.2 are in the localization $\mathcal{R}_P \subseteq \mathcal{O}'_P$.

Basis $\{b_i\} = \{(\alpha^{k_P}\pi^{j_P})^i\}$**:**

$$\begin{aligned}(\alpha^{k_P}\pi^{j_P})^i &= \alpha^{k_{P,i}}\alpha^{t_{P,i}n}\pi^{j_P i}\\ &= \alpha^{k_{P,i}}u^{t_{P,i}}\pi^{j_P i} \text{ where } u = \pi^{v_P(u)}u'\\ &= \omega_{k_{P,i}}u'^{t_{P,i}}\pi^{v_P(u)t_{P,i}+j_P i}\\ &= u'^{t_{P,i}}r \text{ where } r \in R \text{ since } \pi^{v_P(u)t_{P,i}+j_P} \in \mathfrak{a}_i\end{aligned}$$

Since $v_P(u') = 0$, $v_P(u'^{t_{P,i}}) = 0$ also, so there is no P in the denominator of $(\alpha^{k_P}\pi^{j_P})^i$. Therefore $(\alpha^{k_P}\pi^{j_P})^i \in \mathcal{R}_P$.

Basis $\{b_{il}\} = \{(\alpha^{n/g_P}\pi^{-v_P(u)/g_P})^i(\alpha^{k_P}\pi^{j_P})^l\}$**:**

$$\begin{aligned}(\alpha^{n/g_P}\pi^{-v_P(u)/g_P})^i(\alpha^{k_P}\pi^{j_P})^l &= \alpha^{in/g_P+k_P l}\pi^{-iv_P(u)/g_P+j_P l}\\ &= \alpha^{k_{P,il}}\alpha^{t_{P,il}n}\pi^{-iv_P(u)/g_P+j_P l}\\ &= \alpha^{k_{P,il}}u^{t_{P,il}}\pi^{-iv_P(u)/g_P+j_P l}\\ &= \omega_{k_{P,il}}u'^{t_{P,il}}\pi^{-iv_P(u)/g+j_P l+v_P(u)t_{P,il}}\\ &= u'^{t_{P,il}}r \text{ where } r \in R \text{ since } \pi^{-iv_P(u)/g_P+j_P l+v_P(u)t_{P,il}} \in \mathfrak{a}_{il}\end{aligned}$$

Since $v_P(u') = 0$, $v_P(u'^{t_{P,il}}) = 0$ also, so there is no P in the denominator of $(\alpha^{n/g_P}\pi^{-v_P(u)/g_P})^i(\alpha^{k_P}\pi^{j_P})^l$. Therefore $(\alpha^{n/g_P}\pi^{-v_P(u)/g_P})^i(\alpha^{k_P}\pi^{j_P})^l \in \mathcal{R}_P$.

The basis $\{(\alpha^{k_P}\pi^{j_P})^i\}_i$ or $\{(\alpha^{n/g_P}\pi^{-v_P(u)/g_P})^i(\alpha^{k_P}\pi^{j_P})^l\}_{il}$ is an integral basis for F' at P, that is, it is a basis for the integral closure $\mathcal{O}'_P$. Therefore the integral closure $\mathcal{O}'_P$ is contained in the localization $\mathcal{R}_P$. Since also the localization $\mathcal{R}_P$ is contained in the integral closure $\mathcal{O}'_P$ the localization $\mathcal{R}_P$ is the integral closure $\mathcal{O}'_P$. Therefore we have that $v(\text{disc}(\mathcal{R}_P)) = v(\text{disc}(\mathcal{O}'_P))$. But by [**PZ89**] p292 (invariance under localization) this means that $v_P(\text{disc}(\mathcal{R})) = v_P(\text{disc}(\mathbb{Z}_{F'}))$ since $\mathcal{O}'_P$ is the localization of $\mathbb{Z}_{F'}$ at P. Therefore $\mathcal{R}$ is P-maximal for all $P \in S$ and so $\mathcal{R}$ is S-maximal and the S-maximal over order of $\mathcal{O}$. □

2.2.2. The Maximal Order.

Algorithm 1 (Compute a maximal order in a radical extension)**.**
Input:

- *An order $\mathbb{Z}_F[\alpha]$ of a radical extension F'/F, with $\alpha^n = u \in F$, where $\mathbb{Z}_F$ is the integral closure of $k[t]$ or V_∞ in F.*

Output:

- *The maximal order of $\mathbb{Z}_F[\alpha]$ over $\mathbb{Z}_F$.*

STEPS:

1. *Compute the set S of primes of $\mathbb{Z}_F$ at which u has positive valuation and n has valuation 0.*
2. *Compute the S-maximal over order $\mathcal{S}$ of $\mathbb{Z}_F[\alpha]$ with pseudo basis $(\omega_i, \mathfrak{a}_i)_{0\leq i<n}$ given in Proposition 2.4.*
3. *If F is a number field compute the set of primes $S_C \subset \mathbb{P}_F$ where n has positive valuation. Compute the S_C-maximal order of $\mathbb{Z}_F[\alpha]$ using another algorithm, see Section 2.4.*
4. *Return the sum of $\mathcal{S}$ and the S_C-maximal order computed in Step 3. These orders may be added as modules since the indices of $\mathbb{Z}_F[\alpha]$ in these orders are coprime.*

Theorem 2.6. *The order computed by Algorithm 1 is the maximal order of F'/F containing $\mathbb{Z}_F$.*

Proof. Let $\mathcal{R} = \mathcal{R}_S + \mathcal{R}_C$ be the order computed by Algorithm 1. By Theorem 2.5 $\mathcal{R}_S$ is the S-maximal over order of $\mathbb{Z}_F[\alpha]$. We also have that $\mathcal{R}_C$ is S_C-maximal. Since the discriminant of $\mathbb{Z}_F[\alpha]$ is $n^n u^{n-1}$ $S \cup S_C$ contains all primes dividing this discriminant and $\mathcal{R} \supseteq \mathcal{R}_S, \mathcal{R}_C$, $\mathcal{R}$ is the maximal order of F'/F over $\mathbb{Z}_F$. □

2.3. Complexity

We now analyse the complexity of step 2 in Algorithm 1. We compute n powers $P^{\mu_{P,i}}$ for each prime $P \in S$ where $0 \geq \mu_{P,i} = j_P i_P + v_P(u) t_{P i_P} \geq -v_P(u)$ (and similarly for $g_P > 1$) so the powers we compute have exponents between 0 and $-v_P(u)$. If $v_P(u)$ is relatively small we could compute all powers $P^\mu, 0 > \mu \geq -v_P(u)$. Therefore we do at most $\#S \max\{n \log(v_P(u)), v_P(u)\}$ ideal multiplications in F. Computing $v_P(u)$ for all $P \in S$ involves $O(\#S \log(v_P(u)))$ element multiplications in F. Let $v(u)$ be the maximum valuation in u. Then the complexity of computing the pseudo basis in Proposition 2.4 is in $O(\#Sn \log(v(u)) + \#S \log(v(u)))$ which is linear in the degree of the field extension and the number of primes to consider and logarithmic in the maximum valuation of the constant coefficient.

2.4. Critical Primes

We note a limitation of our algorithm for number fields only. Since critical primes do not occur in function fields our algorithm is complete for function fields.

Definition 2.7. *Let P be a place of a number field F and let F' be an extension of F. If the generator of $P \cap \mathbb{Z}$ divides the degree of F'/F then P is a* critical prime *for F'/F.*

The order given in Theorem 2.5 (unlike the order computed using Algorithm 1) is not P-maximal at primes P which are critical primes and not totally ramified. This is because Theorem 2.5 relies on Theorem 2.2 which requires that $v_P(n) = 0$ when P is an unramified or not totally ramified prime. The order it does compute may not be big enough so the Round 2 was called on the result which became very expensive in some examples. This only applies to orders $\mathbb{Z}_F[\alpha]$ which are not maximal since if $\mathbb{Z}_F[\alpha]$ is maximal this can be determined using the Dedekind test [**Coh00**].

In the small number of cases when $F = \mathbb{Q}$, Round 4 can be applied. In the case where F' can be completed we can factorize the defining polynomial of F' over the completion of F at P and use the two-element certificate returned along with the factorization [**Pau01**] to form a matrix over the completion which is mapped back to F and becomes the basis matrix of the P-maximal order. We also compute the exponents for the powers of P which are the coefficient ideals of the P-maximal order.

For number fields of prime degree there are techniques to compute a P-integral basis when P is a critical prime [**Dab95**]. Such techniques could be extended to fields whose degree is the product of 2 primes, however they involve a congruence that is difficult and currently time consuming to solve so we have not done any further work in this direction.

2.5. Other Uses of the Algorithm

There are some maximal order computations other than maximal orders of radical extensions which we hoped could benefit from the use of Algorithm 1. We identified or constructed Kummer extensions in these computations, computed a pseudo basis for the maximal order in that Kummer extension then mapped that maximal order basis back to the original extension. This was found to be very advantageous for computing maximal orders of class fields of number fields.

2.5.1. Dual and Intersection. Let $\mathcal{O} = \mathbb{Z}_F[\alpha]$ be an order in the field extension F'/F of degree n. Let $\mathcal{O}^\#$ denote the dual of $\mathcal{O}$ with respect to the trace and let K be an extension containing F'. Once we have a maximal order for K we need to intersect that maximal order with F' to gain a maximal order of F' since K is larger than F'. To do this we compute the dual of $\mathcal{O}$ in the original field F' where the dual is defined as

$$\mathcal{O}^\# = \{x \in F' | \mathrm{Tr}(x\mathcal{O}) \in \mathbb{Z}_F\}.$$

For all $x \in \mathbb{Z}_{F'}$ we have $xe \in \mathbb{Z}_{F'}$ for all $e \in \mathcal{O}$ so $x \in \mathcal{O}^{\#}$ and $\mathbb{Z}_{F'} \subseteq \mathcal{O}^{\#}$. Note that this holds for all orders of F'.

In parallel to Cohen [**Coh00**] Definition 2.3.16 and Proposition 2.3.18 and more generally we have

Proposition 2.8. *Let $(\omega_i, \mathfrak{a}_i)_i$ be a pseudo basis of an order $\mathcal{O} \subset F'/F$ where $\omega_i \in F'$ and $\mathfrak{a}_i$ are fractional ideals of $\mathbb{Z}_F$. If $T = \mathrm{Tr}_{F'/F}(\omega_i\omega_j)$, the pseudo matrix $[(\mathfrak{a}_i^{-1})_i, T^{-1}]$ represents a pseudo basis of $\mathcal{O}^{\#}$.*

The proof follows similarly to Cohen's proof of Proposition 2.3.18 in [**Coh00**].

We only compute the pseudo basis of the module $\mathcal{O}^{\#}$ and not the module itself, as it is sufficient and more efficient to work with the pseudo basis only. To compute the intersection of the integral closure of $\mathbb{Z}_F$ in $K \supset F'$ with $\mathcal{O}^{\#}$, we calculate a pseudo basis of the integral closure of $\mathbb{Z}_F$ in K with coefficient ring $\mathbb{Z}_F$. We consider the pseudo basis of $\mathcal{O}^{\#}$ as pseudo elements of K and use these two pseudo bases to compute the intersection of the modules with these bases. Using the pseudo basis of the intersection we construct the maximal order of F' as a transformation of $\mathcal{O}$.

2.5.2. A Kummer approach to Radical Extensions. We began by following a similar approach to [**Dab95**], Section 4.3. For a radical extension F'/F of degree n we computed a cyclotomic extension F_c/F, a field extension whose defining polynomial is a cyclotomic polynomial with roots the primitive nth roots of unity ([**vdW66**], p. 113–114), and extended this by the defining polynomial of F'/F to gain a Kummer extension K/F_c. After computing the maximal order of K using Algorithm 1 we intersected this with $\mathbb{Z}_F[\alpha]^{\#} \subset F'$ to gain the maximal order of F'/F.

Unfortunately this was quite expensive for some examples, in particular those for which $[F_c : F]$ was almost equal to $[F' : F]$. However, [**Sti93**] Remark III.7.5 notes that he does not use the presence of the roots of unity in the coefficient field. So we stated Theorem 2.2 and Algorithm 1 for radical extensions rather than Kummer extensions.

It turns out that the algorithm following [**Dab95**] can be faster than Round 2 for some examples requiring only small degree cyclotomic extensions but Algorithm 1 is faster still. For a comparison of timings see Section 2.7.4.

2.5.3. Using Algorithm 1 to Compute Maximal Orders of Class Fields. A similar approach can be taken to compute maximal orders of class fields. Here we can decompose the field into a compositum of cyclic fields C_i/F of prime power degree l^r. A generator β_i inside a Kummer extension can be found for each C_i whose degree is coprime

to the characteristic so there is known a Kummer extension $K_i = F(\zeta_{lr})(\beta)$ and some $\alpha_i \in K_i$ such that $C_i = F(\alpha_i)$. We compute the maximal order of each Kummer extension K_i then intersect this with the dual of the order $\mathbb{Z}_F[\alpha]$ in the class field C_i to gain a maximal order, as explained in Section 2.5.1.

Algorithm 2 (Compute a maximal order of a class field using a Kummer extension)**.**
Input:

- *An abelian field A/F of characteristic p*

Output:

- *A maximal order of the abelian field A/F*

Steps:

1. *For each cyclic field component $C/F = F(\alpha)$ of A/F do*
   (a) *if $p \nmid \deg(C)$ or $p = 0$*
      (i) *Retrieve the associated Kummer extension $K/F(\zeta)/F$ of C.*
      (ii) *If C is a Kummer extension then compute the maximal order of C using Algorithm 1.*
      (iii) *Otherwise*
         (A) *Construct a Kummer extension K_a isomorphic to K but defined as an extension of $F(\zeta)$ represented as an extension of $\mathbb{Q}$ or $\mathbb{F}_q(t)$.*
         (B) *Compute the maximal order of K_a using Algorithm 1.*
         (C) *Find a pseudo basis of the maximal order of K_a with respect to $F(\zeta)$. This is a pseudo basis for the maximal order of K.*
         (D) *Find a basis for the dual of $\mathbb{Z}_F[\alpha] \subset C$.*
         (E) *Take the intersection of the pseudo bases in 1(a)iiiC and 1(a)iiiD and construct the (mostly) maximal order $\mathcal{M}$ of C with this pseudo basis.*
      (iv) *If there are critical primes which are not totally ramified in the discriminant of K then we do not handle them in Algorithm 1 so $\mathcal{M}$ is not maximal and we handle all the critical primes as discussed in Section 2.4 to get the maximal order of C.*
   (b) *otherwise compute the maximal order of the Artin–Schreier–Witt extension C.*
2. *The maximal orders of the components C are then combined together* [**Fie02**]*. Since it is easy to compute the discriminant of A from the class field theoretic input it is easy to determine whether this order is maximal and if it is not to compute its*

maximal order using the algorithm of [**BL94**] *which requires information about the discriminant to be known or Round 2.*

2.6. Examples

We show calculations for a few simple examples. The first example has one ramified and one unramified prime.

Example 1. *Consider* $K/\mathbb{Q}$ *given by* $K = \mathbb{Q}[x]/\langle x^2 + 11\rangle, u = 11$. *There are* 2 *primes dividing the discriminant* -44 *of the equation order of* K. *The prime* 2 *is critical and does not ramify in* K, *the prime* 11 *ramifies in* K. *We have* $v_2(u) = 0$ *and* $v_{11}(u) = 1$. *At the prime* 2 *we have* $g = 0, k = 1, j = 0$. *At the prime* 11 *we have* $g = 1, k = -1, j = 1$. *So we have an* 11*-integral basis* $\{(\alpha^{-1}11)^i\}_{i=0,1}$ *where* $\alpha^2 = 11$. *Note that* $\{\alpha^i\}_{i=0,1}$ *is integral at* 2 *but is not a* 2*-integral basis. We compute the pseudo basis* $\{(1,1),(\alpha,11^{1-1})\}$ *at* 11 *using* $k_0 = 0, t_0 = 0, k_1 = 1, t_1 = -1$. *The methods in this chapter allow us to compute the basis* $\{\alpha^i\}_i$ *for the* 11*-maximal order but not for the* 2*-maximal order since* 2 *is a critical prime. Now that the* 11*-maximal order is known we only need to compute a 2-maximal order using the Round* 4 *algorithm.*

We give an example of a function field which is a Kummer extension. This example contains primes which are neither totally ramified nor unramified.

Example 2. *Consider* $F/\mathbb{Q}(\zeta_8)(t) = \mathbb{Q}(\zeta_8)(t)(\alpha)$ *given by* $F = \mathbb{Q}(\zeta_8)(t)[x]/\langle x^8 + 3t^4\rangle$. *There is* 1 *prime dividing each of the discriminants of* $\mathbb{Q}(\zeta_8)[t][\alpha]$ $(36691771392t^{28})$ *and* $\mathbb{Q}(\zeta_8)[1/t][\gamma]$ $(36691771392/t^{28})$. *Both primes,* $P = t, 1/t$, *have* $v_P(u) = 4$ *and also* $g = 4$. *Therefore we have a* t*-integral basis* $\{(\alpha^2t^{-1})^i(\alpha^{-1}t)^l\}_{0\le i<4,0\le l<2}$ *and a* $1/t$*-integral basis* $\{(\gamma^2(1/t)^{-1})^i(\gamma^{-1}1/t)^l\}_{0\le i<4,0\le l<2}$ *where* $\alpha^8 = -3t^4$ *and* $\gamma^8 = -3/t^4$. *We compute the pseudo basis*

$$\{(1,t^0),(\alpha^7,t^{-3}),(\alpha^2,t^{-1}),(\alpha,t^0),(\alpha^4,t^{-2}),(\alpha^3,t^{-1}),(\alpha^6,t^{-3}),(\alpha^5,t^{-2})\}$$

at t *and*

$$\{(1,(1/t)^0),(\gamma^7,(1/t)^{-3}),(\gamma^2,(1/t)^{-1}),(\gamma,(1/t)^0),(\gamma^4,(1/t)^{-2}),$$
$$(\gamma^3,(1/t)^{-1}),(\gamma^6,(1/t)^{-3}),(\gamma^5,(1/t)^{-2})\},$$

at $1/t$. *At* t *we form the matrix with diagonal* $[1,1,t^{-1},t^{-1},t^{-2},t^{-2},t^{-3},t^{-3}]$ *as the transformation matrix for the* (t)*-maximal order of* F *as a transformation of* $\mathbb{Q}(\zeta_8)[t][\alpha]$ *having*

basis $\{\alpha^i\}$ *over* $\mathbb{Q}(\zeta_8)[t]$. *At* $1/t$ *we form the matrix with diagonal*

$$[1, 1, (1/t)^{-1}, (1/t)^{-1}, (1/t)^{-2}, (1/t)^{-2}, (1/t)^{-3}, (1/t)^{-3}]$$

as the transformation matrix for the $(1/t)$*-maximal order of* F *as a transformation of* $\mathbb{Q}(\zeta_8)[1/t][\gamma]$ *having basis* $\{\gamma^i\}$.

Note that the calculations here are identical for each prime since they share the same valuation of u *and the rest is substitution of primitive elements and primes.*

The next example is represented as a relative extension. It contains 2 primes which are totally ramified and 5 which are partially ramified.

Example 3. *Consider* F'/F *given by* $F = \mathbb{F}_7(t)[x]/\langle x^3 + x + (t+1)/t^2\rangle, F' = F[x]/\langle x^6 + (t+1)(t+2)^3/t\rangle$. *Let* α *be such that* $\alpha^6 + t^5(t+1)(t+2)^3 = 0$, γ *such that* $\gamma^6 + (t+1)(t+2)^3/t^7 = 0$. *There are 5 primes dividing the discriminant of* $\mathbb{Z}_F^0[\alpha]$ *and 2 primes dividing the discriminant of* $\mathbb{Z}_F^\infty[\gamma]$. *These primes are ideals of either* $\mathbb{Z}_F^0$ *or* $\mathbb{Z}_F^\infty$. *There is 1 prime above* t *and 2 primes above each of* $t+1$ *and* $t+2$, *and we shall call these* $P_0, P_{11}, P_{12}, P_{21}$ *and* P_{22} *respectively. There are 2 primes above* $1/t$ *which we shall call* $P_{\infty 1}$ *and* $P_{\infty 2}$. *We have* $v_{P_0}(u) = 15, v_{P_1}(u) = 1, v_{P_2}(u) = 3$ *and* $v_\infty(u) = 3$ *(the valuation of* u *is the same for both primes lying over* $t+1, t+2$ *and* $1/t$*).*

Let π_r *be a uniformizing element for* P_r. *We compute* $\{(\alpha^2\pi_0^{-5})^i(\alpha\pi_0^{-2})^l\}_{0\le i<3, 0\le l<2}$ *for a* P_0*-integral basis, a* P_{11}*-integral basis* $\{\alpha^i\}$, *a* P_{21}*-integral basis* $\{(\alpha^2\pi_{21}^{-1})^i\alpha^l\}_{0\le i<3, 0\le l<2}$ *and a* $P_{1\infty}$*-integral basis* $\{(\gamma^2\pi_{1\infty}^{-1})^i(\gamma\pi_{1\infty}^0)^l\}_{0\le i<3, 0\le l<2}$. *We note that the* P_{12}*-integral basis differs to the* P_{11}*-integral basis only in the uniformizer, the* P_{22}*-integral basis differs to the* P_{22}*-integral basis only in the uniformizer and the* $P_{\infty 2}$*-integral basis differs to the* $P_{\infty 1}$*-integral basis only in the uniformizer because of their common valuations of* u.

We compute the pseudo bases

$$\{(1,1), (\alpha, P_0^{-2}), (\alpha^2, P_0^{-5}), (\alpha^3, P_0^{-7}), (\alpha^4, P_0^{-10}), (\alpha^5, P_0^{-12})\}, \text{ at } P_0,$$

$$\{(\alpha^i, 1)\}_{0\le i<6} \text{ at } P_{11} \text{ and } P_{12},$$

$$\{(1,1), (\alpha, 1), (\alpha^2, P_2^{-1}), (\alpha^3, P_2^{-1}), (\alpha^4, P_2^{-2}), (\alpha^5, P_2^{-2})\} \text{ at } P_{21} \text{ and } P_{22}$$

and

$$\{(1,1), (\gamma, P_\infty^0), (\gamma^2, P_\infty^{-1}), (\gamma^3, P_\infty^{-1}), (\gamma^4, P_\infty^{-2}), (\gamma^5, P_\infty^{-2})\} \text{ at } P_{\infty 1} \text{ and } P_{\infty 2}$$

where we use the shorthand P_1 *to refer to either* P_{11} *or* P_{12}, P_2 *to refer to either* P_{21} *or* P_{22} *and* P_∞ *to refer to either* $P_{\infty 1}$ *and* $P_{\infty 2}$. *The transformation matrices are identity matrices. The coefficient ideals in the pseudo matrix for* P_0 *are* $[1, P_0^{-2}, P_0^{-5}, P_0^{-7}, P_0^{-10}, P_0^{-14}]$, *for* P_{11}

and P_{12} *are* $[1]_{0\le i<6}$*, for* P_{21} *and* P_{22} *are* $[1, 1, P_2^{-1}, P_2^{-1}, P_2^{-2}, P_2^{-2}]$ *and for* $P_{\infty 1}$ *and* $P_{\infty 2}$ *are* $[1, P_\infty^0, P_\infty^{-1}, P_\infty^{-1}, P_\infty^{-2}, P_\infty^{-2}]$.

2.7. Timings

We give timings showing that Algorithm 1 and Algorithm 2 are faster than previous algorithms for a range of fields. Note that the Round 2 algorithm involves randomness so timings for this algorithm may differ depending on seed.

Timings are given for an Intel(R) Core(TM)2 i7-3770 CPU 3.4GHz (32GB RAM) machine running MAGMA V2.20-8 under Linux.

2.7.1. Maximal Orders of Number Fields. Computing maximal orders of degree n Kummer extensions of the cyclotomic field of order n showed that Algorithm 1 could be 10 times as fast as Round 2 or 4 even for some small examples. A comparison of timings is given in Table 2.1.

$\mathbb{Q}(\zeta_n)/\langle x^n - a\rangle$	Algorithm 1	Round 2 or 4
$x^3 - 5^4$	0.01s	0.02s
$x^6 - 7^5$	0.04s	0.07s
$x^9 - 2^4$	0.22s	2.72s
$x^{12} - 5^7$	0.24s	1.85s

TABLE 2.1. Maximal order computation timings for Kummer extensions of Cyclotomic Fields

2.7.2. Maximal Orders of Function Fields. We give the timings from some simple examples in Table 2.2. We refer to the primes that lie above $1/t$ as infinite primes and those which lie above a polynomial in t as finite primes, as does [**Fra05**]. We give timings for computing orders which are maximal at all finite primes and orders which are maximal at all infinite primes.

We ran a batch of maximal order computations for function fields computed as abelian extensions. Let $F = \mathbb{F}_9(t)[x]/\langle x^3 + x + 1/t + 1/t^2\rangle$. We form a divisor D by adding together some places of F of degree 2, compute its ray class group R and form the quotient Q of R by $8R$. We compute the subgroups of Q and compute an abelian extension for D and each subgroup. Let F_i' be the extension of F defined by the defining polynomial of the ith abelian extension (of degree 8). There were 448 fields F_i'. Some timings for the computations of the finite and infinite maximal orders of F_i' are given in Table 2.3.

Field	Algorithm 1	Round 2
$\mathbb{Q}(\zeta_8)(t)[x]/\langle x^8 - 3t^4\rangle$ (finite)	0.01s	0.02s
$\mathbb{Q}(\zeta_8)(t)[x]/\langle x^8 - 3t^4\rangle$ (infinite)	0.00s	0.06s
$\mathbb{Q}(\zeta_{20})(t)[x]/\langle x^{20} - 7t^{11}\rangle$ (finite)	0.01s	0.72
$\mathbb{Q}(\zeta_{20})(t)[x]/\langle x^{20} - 7t^{11}\rangle$ (infinite)	0.02s	2.18
$\mathbb{Q}(t)(\zeta_7)[x]/\langle x^7 + t\zeta_7\rangle$ (finite)	0.00s	0.03s
$\mathbb{Q}(t)(\zeta_7)[x]/\langle x^7 + t\zeta_7\rangle$ (infinite)	0.01s	121.4s

TABLE 2.2. Maximal order computation timings for Kummer extensions of function fields

	Algorithm 1	Round 2
Maximum time (finite)	0.08s	3.8s
Average time (finite)	0.039s	1.6s
Maximum time (infinite)	0.03s	3.87s
Average time (infinite)	0.008s	0.451s

TABLE 2.3. Maximal order computation timings for Kummer extensions of function fields occurring in abelian extensions

We also ran Algorithm 1 on the Kummer extensions given as examples in [**Fra05**] Section 5.1. In Table 2.4 we give the averages of times from our implementation and that of [**Fra05**] for comparison. [**Fra05**] divided his Kummer extension examples into 3 groups, we compute an average for each of those groups. The first group of examples are of the form $F' = F[y]/\langle y^n - u\rangle$ where $F = \mathbb{F}_q(t)[x]/\langle x^5 + 4x^4 + t^2x^3 + 2x^2 + t^5x + t + 1\rangle$, ρ is a primitive element of F, q is a power of 5 and

$$u = \frac{t^{11} + 4t^{10} + t^8 + 4t^7 + t^5 + 4t^4 + t^2 + 4t + 1}{t^4 + 4t^3 + t + 4}\rho^4 + \frac{1}{t^2 + 3}\rho + t^2.$$

The second group are of the form $F' = F[y]/\langle y^n - u\rangle$ where $F = \mathbb{F}_q(t)[x]/\langle x^2 + 2x + t^3 + t + 1\rangle$, ρ is a primitive element of F, q is a power of 3 and $u = 1/t^2\rho + t^2$. The third group are of the form $F' = F[y]/\langle y^n - u\rangle$ where $F = \mathbb{F}_q(t)[x]/\langle x^3 - (t+1)x^2 + 2tx - t^5\rangle$, ρ is a primitive element of F, q is a power of 3 and $u = (t^3 + 2)\rho^2 + (t^2 + 1)\rho + 1$. [**Fra05**] gave timings for finite maximal order computations for the first and second group of examples and timings for infinite maximal order computations for the third group of examples. We will do likewise. Since we cannot reproduce or better the timings given in [**Fra05**] when running an implementation of his algorithm for group 2 we give an average of the times

given in [**Fra05**] in brackets. Using Round 2 example 11 took over 32 hours. We did not attempt the rest of the examples in this group using Round 2.

Examples	n	Algorithm 1	Round 2	[**Fra05**]
1 – 6	11 – 24	0.92s	458.187s	73.48s
7 – 14	28 – 160	121.023s	1.2hrs (e.g. 7 – 10 only)	1065.911s (805s)
15 – 20	5 – 29	0.198s	115.342s	3.455s

TABLE 2.4. Comparison of average times for examples from [**Fra05**]

2.7.3. Maximal Orders of Abelian Fields. Let $F = \mathbb{Q}[x]/\langle x^2 - 2\rangle$. We compute the ray class group R of a divisor of F and take the quotient Q of R by nR where n will be the degree of the resulting number fields. For the subgroups S of Q such that Q/S is cyclic of order n we compute an abelian extension A and compute the maximal order of A using both Algorithm 2 and the Round 2 algorithm. Some average times are given in Table 2.5.

Degree	Algorithm 2	Round 2
8	0.176s	4.614s
9	0.577s	33.373s
11	4.432s	349.133s
16	8.86s	36.3min

TABLE 2.5. Comparison of average timings of maximal order computations for abelian fields

In [**Fie06**] Section 3.4 there is a genus computation which took almost 2.5hrs in MAGMA V2.11 on a 64-bit 2.6GHz AMD processor. This computation currently takes around 0.03s using the techniques described in this chapter but took 2000s in MAGMA V2.12 using the same machine used for our timings.

2.7.4. Maximal Orders of Radical Extensions. We compare times of implementations of Algorithm 1, Round 2 and the approach similar to [**Dab95**] for radical extensions in Tables 2.6 and 2.7, as much as practical.

In Table 2.7 we use extensions of $\mathbb{F}_{101}(t)[y]/\langle y^3+y^2+y+t\rangle$ of a range of degrees and give average times for 10 random radical extensions of each degree whose defining polynomials are of the form $x^n - \prod_{i=1}^{3} p_i^{e_i}$, where p_i is a random prime polynomial and e_i is a random integer in the range $[1 \ldots 5]$ randomly multiplied by either 1 or 2.

Extension	Algorithm 1	Round 2	Section 2.5.2
$\mathbb{Q}(t)(\sqrt{-t})[x]/\langle x^{12}+\sqrt{-t}\rangle$ (finite)	0.00s	0.07s	0.04s
$\mathbb{Q}(t)(\sqrt{-t})[x]/\langle x^{12}+\sqrt{-t}\rangle$ (infinite)	0.02s	7.83s	0.57s
$\mathbb{Q}(t)(\sqrt{-t})[x]/\langle x^{13}+\sqrt{-t}\rangle$ (finite)	0.01s	0.09s	307.31s
$\mathbb{Q}(t)(\sqrt{-t})[x]/\langle x^{13}+\sqrt{-t}\rangle$ (infinite)	0.02s	10.97s	1403.08s
$\mathbb{F}_{101}(t)(\sqrt{-t})[x]/\langle x^{13}+\sqrt{-t}\rangle$ (finite)	0.01s	0.01s	0.04s
$\mathbb{F}_{101}(t)(\sqrt{-t})[x]/\langle x^{13}+\sqrt{-t}\rangle$ (infinite)	0.03s	9.58s	1.29s

Table 2.6. Comparison of timings for maximal order computations of radical extensions

Degree	Algorithm 1	Round 2	Section 2.5.2
11 (finite)	0.068s	9.262s	78.975s
11 (infinite)	0.095s	6.864s	1332.542s
12 (finite)	0.03s	14.062s	0.142s
12 (infinite)	0.118s	15.558s	0.343s
13 (finite)	0.095s	17.8s	20.279s
13 (infinite)	0.115s	16.107s	22.185s
14 (finite)	0.039s	25.618s	5.819s
14 (infinite)	0.128s	31.715	24.248s
15 (finite)	0.074s	29.754s	0.423s
15 (infinite)	0.133s	32.746s	0.354
19 (finite)	0.214s	75.529s	124.325s
19 (infinite)	0.198s	124.045s	692.972s
21 (finite)	0.210s	119.297s	45.991
21 (infinite)	0.231s	205.433s	26.589s
22 (finite)	0.086s	155.576s	82.259s
22 (infinite)	0.239s	271.019s	1418.989s
23 (finite)	0.194s	175.341s	93.015s
23 (infinite)	0.247s	323.078s	59mins
27 (finite)	0.45s	394.033s	37mins
27 (infinite)	0.312s	763.218s	>7hrs
28 (finite)	0.125s	475.416s	28.510s
28 (infinite)	0.342s	934.474s	33.795s
29 (finite)	0.39s	535.519s	>2.9hrs
29 (infinite)	0.49s	1293.871s	>8.4hrs
30 (finite)	0.112s	648.358s	1.683s
30 (infinite)	0.378s	1206.643s	4.597s
31 (finite)	0.409s	727.231s	49.639s
31 (infinite)	0.468s	1440.772s	19.653s

Table 2.7. Comparison of average timings for maximal order computations of radical extensions

Chapter 3

Artin–Schreier Extensions

In characteristic p there are no Kummer extensions of any degree divisible by p because any polynomial $x^n - u$ where $p \mid n$ is not separable. In order to construct cyclic extensions of degree p of a characteristic p function field we instead use Artin–Schreier extensions. These extensions are cyclic Galois extensions whose automorphisms are given by $\alpha \mapsto \alpha + \lambda, \lambda = 0, \ldots, p-1$ where α is a root of the defining polynomial of the extension. Artin–Schreier extensions have a notion of equivalence parallel to that of Kummer equivalence. We can construct an isomorphic Artin–Schreier extension whose defining polynomial has constant coefficient with positive valuation or valuation coprime to p at any given primes. A root of the defining polynomial of the isomorphic extension generates a P-integral power basis for the extension when P is an unramified prime.

Definition 3.1 ([**Sti93**] Proposition III.7.8)**.** *Let F be a function field of characteristic $p > 0$ with perfect constant field and let $u \in F$ be such that $u \neq w^p - w$ for all $w \in F$. Then $F' = F(\alpha)$ where $\alpha^p - \alpha = u$ is an* Artin–Schreier *extension of F.*

In the case of Kummer extensions we presented a pseudo basis for the more general case of radical extensions. In the case of Artin–Schreier extensions we could state the pseudo basis for some more general extensions defined by an additive separable polynomial $a(T) = \sum_i^n a_i T^{p^i} = u$ ([**Sti93**] Proposition III.7.10). We use properties of these extensions which are not true in general in order to compute our pseudo bases.

The results in this chapter also appear in [**Sut13**].

3.1. Artin–Schreier Quotients

Our computations rely heavily on some specific elements we describe in this section.

Definition 3.2. *Let F be a function field of characteristic $p > 0$ with separable closure $\bar{F}$. The* Artin–Schreier operator *$\wp : \bar{F} \to \bar{F}$ is the $\mathbb{F}_p$-linear homomorphism $\wp : x \mapsto x^p - x$.*

Let $P \in \mathbb{P}_F$ and $u \in F$. An Artin–Schreier quotient *of u modulo P is an element $z_P \in F$ satisfying $v_P(u - \wp(z_P)) \geq 0$ or $p \nmid v_P(u - \wp(z_P)) < 0$.*

Let $S \subset \mathbb{P}_F$. If z is an Artin–Schreier quotient of u modulo P for all $P \in S$ then we call z an Artin–Schreier quotient *of u modulo S.*

The quotient terminology is because z can be considered a quotient with respect to the Artin–Schreier operator $\wp$ and $u - \wp(z)$ the corresponding remainder. Note that if $v_P(u - \wp(z_P)) \geq 0$ for an Artin–Schreier quotient z_P of u modulo P then P is unramified and if $v_P(u - \wp(z_P)) < 0$ then P is totally ramified ([**Sti93**] Proposition III.7.8).

We will now give algorithms which compute Artin–Schreier quotients modulo a place P and a set of places S. When F has a perfect constant field these prove that such quotients always exist. The following is Algorithm 3.2.2 (Reduction) of [**Fra05**].

Algorithm 3 (Compute an Artin–Schreier quotient modulo P)**.**
Input:

- *A function field F with perfect constant field, an element $u \in F$ and $P \in \mathbb{P}_F$.*

Output:

- *An Artin–Schreier quotient z_P of u modulo P.*

Steps:

1. *Compute $v_u = v_P(u)$, initialize $z_P = 0, u_z = u$, set r, s such that $v_u = rp + s, 0 \leq s < p$ and set π to a prime element of P.*
2. *while $s = 0$ and $v_u < 0$ do*
   (a) *Compute a as the pth root of the image of $u_z \pi^{-v_u}$ under the residue class map at P.*
   (b) *Replace z_P with $z_P + a\pi^r$.*
   (c) *Replace u_z with $u_z - \wp(a\pi^r)$ and v_u with $v_P(u_z)$.*
   (d) *Recompute r, s such that $v_u = rp + s$.*
3. *Return z_P and* $\min\{v_u, 0\}$.

Note that if the constant field of F is not perfect then we are not guaranteed to be able to compute a p-th root in Step 2a.

Lemma 3.3. *Algorithm 3 terminates with z_P as required.*

Proof. If this algorithm terminates then we obviously have a z_P as required. We explain here why the algorithm terminates. Each time through the loop we effectively remove the first term in the π-adic expansion of u_z at P so each time through the loop v_u is increased by at least 1 and so must eventually become positive. However on entering the loop v_u is

a multiple of p, increasing v_u by anything other than a multiple of p will make s non zero and the loop terminates. □

Algorithm 4 (An extension of the Chinese Remainder Theorem)**.**
Input:

- *A list of places* $P_1, \ldots, P_r \in \mathbb{P}$ *where* $\mathbb{P} = \mathbb{P}_F^0$ *or* $\mathbb{P}_F^\infty$ *and a list of elements* $z_1, \ldots, z_r \in F$.

Output:

- *An element* $z \in F$ *such that* $v_{P_j}(z - z_j) \geq 1, 1 \leq j \leq r$ *and* $v_Q(z) \geq 0$ *for* $Q \in \mathbb{P}, Q \notin \{P_1, \ldots, P_r\}$.

Steps:

1. *Using the CRT compute an element* $z^{(r)}$ *such that* $v_{P_j}(z - z_j) \geq 1$ *for all* $1 \leq j \leq r$. *To do so we initialize* $z^{(1)}$ *to* z_1 *then compute*

$$z^{(j)} = z^{(j-1)} + (z_j - z^{(j-1)})c_j, 1 < j \leq r$$

where

$$1 = c_j + d_j, c_j \in M_{j-1}, d_j \in P_j^{1-\min\{v_{P_j}(z_j - z^{(j-1)}),0\}}$$

and

$$M_j = \prod_{i=1}^{j} P_i^{1-\sum_{l=i}^{j}\min\{v_{P_i}(z_{l+1}-z^{(l)}),0\}}$$

2. *Compute the denominator* d_z *of* $z^{(r)}$ *with respect to* $\mathbb{P}$ *and find those prime factors* $(d_z)_i$ *of* d_z *which have zero valuation at all* $P_j, 1 \leq j \leq r$.
3. *To compute* z *such that* $v_Q(z) \geq 0$ *for* $Q \in \mathbb{P}, Q \notin \{P_1, \ldots, P_r\}$ *also, compute*

$$z^{(j)} = z^{(j-1)} - c_j z^{(j-1)}, r \leq j < r + \#\{(d_z)_i\}$$

where

$$1 = c_j + d_j, c_j \in M_{j-1}, d_j \in (d_z)_{j-r}^{v_{(d_z)_j}(d_z)}\mathbb{Z}_F,$$

where $\mathbb{Z}_F$ *is the maximal order of* F *corresponding to* $\mathbb{P}$ *and*

$$M_j = M_r \prod_{l=1}^{r} P_l^{v_{P_l}(d_z)} \prod_{l=1}^{j-r} (d_z)_l^{v_{(d_z)_l}(d_z)}.$$

Theorem 3.4. *Algorithm 4 produces an element* z *satisfying the output conditions.*

Proof. Let z be the output of Algorithm 4. It can be shown by induction that $v_{P_j}(z - z_j) \geq 1, 1 \leq j \leq r$ since this holds for $z^{(r)}$ by the chinese remainder theorem in Step 1. To see that $v_Q(z) \geq 0$ for $Q \in \mathbb{P}, Q \notin \{P_1, \ldots, P_r\}$, note that $z = \prod_i d_i z^{(r)}$. If $v_Q(d_z) = 0$ then $v_Q(z) = v_Q(z^{(r)}) \geq 0$ and if $v_Q(d_z) \geq 0$ then $v_Q((d_z)_i) \neq 0$ for one i so $v_Q(z) = v_Q(d_i) + v_Q(z^{(r)}) = v_Q(d_z) + v_Q(z^{(r)}) \geq 0$. □

We can use either the Chinese remainder theorem above or strong approximation ([**Fra05**] Algorithm 1.3.3) to compute an Artin–Schreier quotient modulo a set of primes from quotients modulo a single prime. We use the extension of the Chinese remainder theorem (Algorithm 4) because in characteristic less than about 50 the Magma implementation has been seen to be faster than the Magma implementation of strong approximation described in [**Fra05**]. We require the extension to the theorem which removes denominators outside S because we do not want to introduce any new ramification at other primes. The denominator d_z needs to be in $k(t)$ for efficiency.

Algorithm 5 (Compute an Artin–Schreier quotient modulo S)**.**
Input:

- *A function field F with perfect constant field, an element $u \in F$ and a set $S \subset \mathbb{P}_F$.*

Output:

- *An Artin–Schreier quotient z of u modulo S such that $v_Q(z) \geq 0$ for $Q \notin S \cup \{X\}$, for some $X \notin S$.*

Steps:

1. *Compute z_P for all $P \in S$ by Algorithm 3.*
2. *Use strong approximation or the extension to the Chinese remainder theorem (Algorithm 4) to compute z such that $v_P(z - z_P) \geq 1, P \in S$ and $v_Q(z) \geq 0$ for $Q \notin S \cup \{X\}$.*

We note that there may be a place $X \in \mathbb{P}_F, X \notin S$ such that $v_X(z) < 0$. This exceptional place is chosen and can be any place (or places) not in S. We use this algorithm with $S \subset \mathbb{P}$ where $\mathbb{P} = \mathbb{P}_F^0$ or $\mathbb{P}_F^\infty$ and $X \notin \mathbb{P}$.

Lemma 3.5. *Algorithm 5 terminates with z as required.*

Proof. By strong approximation or Chinese remaindering we have that $v_Q(z) \geq 0$ for $Q \notin S \cup \{X\}$. It remains to prove that z is an Artin–Schreier quotient of u modulo S. Let

$P \in S$, then

$$\begin{aligned} v_P(u - \wp(z)) &= v_P(u - \wp(z) - \wp(z_P) + \wp(z_P)) \\ &= v_P(u - \wp(z_P) - (\wp(z) - \wp(z_P))) \\ &\geq \min\{v_P(u - \wp(z_P)), v_P((z - z_P)^p - (z - z_P))\} \\ &\geq \min\{v_P(u - \wp(z_P)), v_P(z - z_P)\} \\ &\geq \min\{v_P(u - \wp(z_P), 1\}. \end{aligned}$$

If $v_P(u - \wp(z_P)) < 0$, $v_P(u - \wp(z)) = v_P(u - \wp(z_P)) = -m < 0, m \not\equiv 0 \mod p$. If $v_P(u - \wp(z_P)) \geq 0$, $v_P(u - \wp(z)) \geq 0$. Hence z is an Artin–Schreier quotient of u modulo S. □

3.2. A P-integral Power Basis

We now consider a P-integral power basis of an Artin–Schreier extension. This we can deduce using [**Sti93**] Proposition III.7.8 (and its proof).

Theorem 3.6. *Let F'/F be an Artin–Schreier extension defined by the polynomial $x^p - x - u$ and let α be a root of this polynomial, a primitive element for F'/F. Let P be a place of F and z an Artin–Schreier quotient of u modulo P.*

unramified: *If P is unramified in F'/F set $k_P = 1, l_P = 0$.*

ramified: *If P is totally ramified in F'/F set l_P, k_P such that $pl_P + v_P(u - \wp(z))k_P = 1$ and $0 \leq k_P < p$. This is possible since $p \nmid v_P(u - \wp(z))$ and k_P and l_P can be adjusted so that $0 \leq k_P < p$.*

Then $\{(\pi^{l_P}(\alpha - z)^{k_P})^j\}_{0 \leq j < p}$ is a local P-integral basis for F' at P, where π is a prime element of P.

Remark 3.7. [**Sti93**] *Proposition III.7.8 also states the different exponents of ramified primes in Artin–Schreier extensions as $(p-1)(-v_P(u - \wp(z)) + 1)$.*

Proof. In both cases we have that $\alpha - z$ is a root of the polynomial $\phi(x) = x^p - x - (u - \wp(z))$. Let P' be a prime of F' such that $P' \mid P$. Suppose that $P' \mid P$ is unramified. Then $v_P(u - \wp(z)) \geq 0$ ([**Sti93**] Theorem III.7.8) so the minimal polynomial $\phi(x)$ of $\alpha - z$ is integral at P. Let $\phi'(x)$ be the derivative of $\phi(x)$. Then $\phi'(x) = -1$ so $v_{P'}(\phi'(\alpha - z)) = 0$, therefore by [**Sti93**] Corollary III.5.11 $\{(\alpha - z)^j\}_{0 \leq j < p}$ is a P-integral basis for F'/F.

Now suppose that $P' \mid P$ is totally ramified, so $p \nmid v_P(u - \wp(z)) < 0$ ([**Sti93**] Theorem III.7.8). Then

$$v_{P'}(\pi^{l_P}(\alpha - z)^{k_P}) = l_P p + k_P v_{P'}(\alpha - z) = l_P p + k_P p v_P(u - \wp(z))/p = 1.$$

So $\pi^{l_P}(\alpha - z)^{k_P}$ is a P'-prime element and so by [**Sti93**] Proposition III.5.12, $\{(\pi^{l_P}(\alpha - z)^{k_P})^j\}_{0 \le j < p}$ is a P-integral basis for F'/F. □

If $v_P(u - \wp(z)) > 0$ then the defining polynomial $x^p - x - (u - \wp(z))$ of an extension isomorphic to F'/F maps to $x^p - x$ under the residue class map at P which is a reducible polynomial and so P splits in F'/F. However if $v_P(u - \wp(z)) = 0$ then P is inert in F'/F.

If $v_P(u - \wp(z)) > 1, z + 1 + \pi$ where π is a prime element of P is also an Artin–Schreier quotient modulo P since

$$\begin{aligned} v_P(u - \wp(z + 1 + \pi)) &= v_P(u - \wp(z) - 1 - \pi^p + 1 + \pi) \\ &\ge \min\{v_P(u - \wp(z)), 1\} \end{aligned}$$

We also have $v_{P'}(\alpha - (z + 1 + \pi)) \ge \min\{v_{P'}(\alpha - z), v_{P'}(1 + \pi)\} = 0$ where the inequality becomes equality so long as $v_{P'}(\alpha - z) > 0$. This is why we used ≥ 1 in Algorithm 5.

However, $\pi^{l_P}(\alpha - z)^{k_P}$ is only guaranteed to be integral at $P' \mid P$. We often require a basis which is integral at more than one place. [**Fra05**] describes a method of scaling elements such that they still generate a power basis for the integral closure $\mathcal{O}'_P$ but are also integral elsewhere. As discussed in Section 1.4.1 we compute a pseudo basis instead.

3.3. A Pseudo Basis

In this section we will consider an Artin–Schreier extension F'/F with defining polynomial $x^p - x - u$ and primitive element α, a root of the defining polynomial.

Let $\mathbb{Z}_F$ be the integral closure of $k[t]$ or V_∞ in F. We start with an order $\mathcal{O} = \mathbb{Z}_F[d\alpha]$ where $d \in \mathbb{Z}_F \cap k(t), v_{P'}(d\alpha) \ge 0$ and is minimal for all $P' \mid P$, P a prime ideal of $\mathbb{Z}_F$.

Theorem 3.8. *Let F'/F be an Artin–Schreier extension, $\mathcal{O} = \mathbb{Z}_F[d\alpha]$ an order of F', S be a set of primes of $\mathbb{Z}_F$ and $z \in F$ an Artin–Schreier quotient of u modulo S. Then*

$$(\omega_j, \mathfrak{a}_j)_j = \left((d(\alpha - z))^j, \prod_{P \in S} P^{\mu_{P,j} - j v_P(d)} \right)_{0 \le j < p},$$

is a pseudo basis over $\mathbb{Z}_F$ for an S-maximal over order of $\mathcal{O}$, where $\mu_{P,j}$ is the smallest non-negative integer such that $v_{P'}(\mathfrak{a}_j \omega_j) \ge 0$ for all $P' \mid P$.

Remark 3.9. *For $P' \mid P$, to have $v_{P'}(\mathfrak{a}_j\omega_j) \geq 0$ we need $v_{P'}(P)(\mu_{P,j} - jv_P(d)) \geq -jv_{P'}(d(\alpha - z))$. If $P' \mid P$ is totally ramified then $\mu_{P,j}p \geq -jv_P(u - \wp(z))$. If $P' \mid P$ is unramified then we need $\mu_{P,j} \geq -jv_P(u - \wp(z)) \leq 0$ so $\mu_{P,j} = 0$. In general, we take*

$$\mu_{P,j} = \max\{\left\lceil \frac{(-jv_P(u - \wp(z)))}{v_{P'}(P)} \right\rceil, 0\}.$$

Note that $\mu_{P,j}$ will be non-zero at only finitely many places of F.

Corollary 3.10. *In the situation of Theorem 3.8, let $\mathbb{P} = \mathbb{P}_F^0$ or $\mathbb{P}_F^\infty$, let S contain all primes $P \in \mathbb{P}$ such that $v_P(d) > 0$, then the S-maximal over order of $\mathcal{O}$ is the maximal order of F' over $\mathbb{Z}_F$ and coincides with the integral closure $\mathcal{O}'_{\mathbb{P}}$ of $\mathcal{O}_{\mathbb{P}}$ in F'.*

Corollary 3.10 applies when S contains all the places occurring in the discriminant of $\mathcal{O}$.

Proof of Theorem 3.8. Let $\mathcal{R}$ be the module with pseudo basis $(\omega_j, \mathfrak{a}_j)_j$ over $\mathbb{Z}_F$. We prove that $\mathcal{R}$ is an order over $\mathbb{Z}_F$, $\mathcal{R}$ contains $\mathbb{Z}_F[d\alpha]$ and $\mathcal{R}$ is S-maximal.

Proof that $\mathcal{R}$ is an order over $\mathbb{Z}_F$: For $j = 0, \omega_0 = 1, \mu_{P,0} = 0$ so $\mathfrak{a}_0 = 1$ and $1 \in \mathcal{R}$.

We now use pseudo elements and check that $\mathfrak{a}_j\omega_j \times \mathfrak{a}_l\omega_l$ is in $\mathcal{R}$. We shall prove that there are integral ideals $\mathfrak{b}, \mathfrak{c}, \mathfrak{d}$ such that

$$\mathfrak{a}_j\omega_j \times \mathfrak{a}_l\omega_l = \begin{cases} \mathfrak{b}\mathfrak{a}_{j+l}\omega_{j+l} & j+l < p \\ \mathfrak{c}\mathfrak{a}_{j+l-p}\omega_{j+l-p} + \mathfrak{d}\mathfrak{a}_{j+l-p+1}\omega_{j+l-p+1} & j+l \geq p. \end{cases} \tag{2}$$
$$\subseteq \mathcal{R}$$

We have

$$\mathfrak{a}_j\omega_j \times \mathfrak{a}_l\omega_l = \mathfrak{a}_j\mathfrak{a}_l\omega_j\omega_l = \mathfrak{a}_j\mathfrak{a}_l\omega_{j+l}$$

and this pseudo element is integral over all $P \in S$ since

$$v_{P'}(\mathfrak{a}_j\omega_j \times \mathfrak{a}_l\omega_l) = v_{P'}(\mathfrak{a}_j\omega_j) + v_{P'}(\mathfrak{a}_l\omega_l) \geq 0$$

holds for $P' \mid P$. For $j + l < p$, this implies $\mu_{P,j} + \mu_{P,l} \geq \mu_{P,(j+l)}$ for all $P \in S$ since $\mu_{P,(j+l)}$ is minimal with this property. Set $\mathfrak{b} = \prod_{P \in S} P^{v_{P\mathfrak{b}}}$ with $v_{P\mathfrak{b}} = \mu_{P,j} + \mu_{P,l} - \mu_{P,(j+l)} \geq 0$. Then $v_Q(\mathfrak{b}) = 0, Q \notin S$, $\mathfrak{b}$ is integral and equation (2) follows in the case $j + l < p$.

For $j+l \geq p$ we make use of

$$\begin{aligned}\omega_p = (d(\alpha - z))^p = d^p(\alpha^p - z^p) &= d^p((\alpha^p - \alpha) - (z^p - z) + \alpha - z) \\ &= d^p((u - \wp(z))) + d^{p-1}\omega_1\end{aligned}$$

and

$$\omega_{j+l} = \omega_{j+l-p}\omega_p = \omega_{j+l-p}d^p(u - \wp(z)) + d^{p-1}\omega_{j+l-p+1}.$$

Then the second case of equation (2) follows with

$$\mathfrak{c} = d^p(u - \wp(z)) \prod_{P \in S} P^{v_{P\mathfrak{c}}}, \quad v_{P\mathfrak{c}} = \mu_{P,j} + \mu_{P,l} - pv_P(d) - \mu_{P,(j+l-p)}$$

and

$$\mathfrak{d} = d^{p-1}(\prod_{P \in S} P^{v_{P\mathfrak{d}}}), \quad v_{P\mathfrak{d}} = (\mu_{P,j} + \mu_{P,l} - (p-1)v_P(d) - \mu_{P,(j+l-p+1)})$$

when we prove the integrality of $\mathfrak{c}$ and $\mathfrak{d}$. To prove $\mathfrak{c}$ is integral, we compute for $P' \mid P \in S$

$$\begin{aligned}&v_{P'}(d^p(u - \wp(z)) \prod_{P \in S} P^{v_{P\mathfrak{c}}}) \\ &= pv_{P'}(d) + v_{P'}(u - \wp(z)) + e(P'|P)(\mu_{P,j} + \mu_{P,l} - pv_P(d) - \mu_{P,(j+l-p)}) \\ &= e(P'|P)(pv_P(d) + v_P(u - \wp(z)) + \mu_{P,j} + \mu_{P,l} - pv_P(d) - \mu_{P,(j+l-p)}) \\ &= e(P'|P)(-\mu_{P,p} + \mu_{P,j} + \mu_{P,l} - \mu_{P,(j+l-p)}) \\ &\geq e(P'|P)(-\mu_{P,p} + \mu_{P,p}) \\ &\geq 0\end{aligned}$$

since

$$\begin{aligned}\mu_{P,(j+l-p)} &= \lceil -(j+l-p)v_P(u - \wp(z))/p \rceil \\ &= \lceil -jv_P(u - \wp(z))/p - lv_P(u - \wp(z))/p \rceil - (-pv_P(u - \wp(z))/p) \\ &\leq \mu_{P,j} + \mu_{P,l} - \mu_{P,p}.\end{aligned}$$

At $Q \notin S, Q \subset \mathbb{Z}_F$,

$$v_Q(d^p(u - \wp(z))) = v_Q\left((d(\alpha - z))^p - d^p(\alpha - z)\right) \geq 0$$

so $\mathfrak{c}$ is integral at all primes of $\mathbb{Z}_F$.

To prove $\mathfrak{d}$ is integral, we have $j+l-p+1 \leq 2p-2-p+1 = p-1$, so

$$(\mathfrak{d}\mathfrak{a}_{j+l-p+1}\omega_{j+l-p+1}) = d^{p-1}\left(\prod_P P^{\mu_{P,j}+\mu_{P,l}-(j+l)v_P(d)}\right)(d(\alpha-z))^{j+l-p+1}$$

and for $P' \mid P \in S$

$$\begin{aligned}
&v_{P'}(\mathfrak{d}\mathfrak{a}_{j+l-p+1}\omega_{j+l-p+1})\\
&= v_{P'}(P)(\mu_{P,j}+\mu_{P,l}-(j+l)v_P(d)) + (j+l)v_{P'}(d) + \\
&\qquad\qquad (j+l-p+1)v_{P'}(\alpha-z)\\
&= v_{P'}(P)\mu_{P,j} + jv_{P'}(\alpha-z) + v_{P'}(P)\mu_{P,l} + lv_{P'}(\alpha-z) + \\
&\qquad\qquad (1-p)v_{P'}(\alpha-z) + (j+l)v_{P'}(d)\\
&\geq 0+0+(1-p)v_{P'}(\alpha-z)+0
\end{aligned}$$

by definition of $\mu_{P,j}$ and $\mu_{P,l}$. For $v_{P'}(\alpha-z) < 0$, $v_{P'}(\mathfrak{d}\mathfrak{a}_{j+l-p+1}\omega_{j+l-p+1}) > 0$ since $(1-p) \leq -1$ and so $\mu_{P,j}+\mu_{P,l} \geq \mu_{P,(j+l-p+1)}$ since $\mu_{P,(j+l-p+1)}$ is minimal with this property. If $v_{P'}(\alpha-z) \geq 0, \mu_{P,j}, \mu_{P,l}, \mu_{P,j+l-p+1} = 0$. In both cases we have $\mu_{P,j}+\mu_{P,l} \geq \mu_{P,(j+l-p+1)}$ and hence $\mathfrak{d}$ is integral. Therefore we have proved equation (2) and $\mathfrak{a}_j\omega_j \times \mathfrak{a}_l\omega_l \subseteq \mathcal{R}$ so $\mathcal{R}$ is a subring and so an order of F'.

Since $\mathcal{R}$ is an order over $\mathbb{Z}_F$ its elements are integral over $\mathbb{Z}_F$.

Proof that Localizations are equal outside of S: To test whether $\mathcal{R}_Q = \mathcal{O}_Q$ for $Q \notin S$ we consider the determinant of the module $\mathcal{R}$, we require this to have valuation 0 for primes Q of $\mathbb{Z}_F, Q \notin S$. The pseudo elements we put in the transformation pseudo matrix are $\mathfrak{a}_j(d(\alpha-z))^j$ which expand to

$$\mathfrak{a}_j\left((d\alpha)^j - \binom{j}{j-1}(d\alpha)^{j-1}(dz) + \ldots + \binom{j}{1}(d\alpha)(-dz)^{j-1} + (-dz)^j\right),$$

where $\binom{j}{i}$ is a binomial coefficient. Since z is in the coefficient ring and the powers of $d\alpha$ are $\leq j$ we have a triangular matrix

$$\begin{pmatrix}
1 & \ldots\ldots\ldots\ldots & 0\\
-dz & 1 \quad \ldots\ldots\ldots\ldots & 0\\
d^2z^2 & 2dz \qquad 1 \quad \ldots. & 0\\
\vdots & \vdots \qquad \vdots \quad \ddots & \vdots\\
d^{p-1}z^{p-1} & -\binom{p-1}{1}d^{p-2}z^{p-2} \quad \binom{p-1}{2}d^{p-3}z^{p-3} \quad \ldots. & 1
\end{pmatrix}$$

with respect to the $d\alpha$ power basis which expresses elements represented with respect to the basis of $\mathcal{R}$ with respect to the basis of $\mathcal{O}$. The determinant is the

product of the diagonal elements which are 1 so the determinant is 1. Multiplying all coefficient ideals we have

$$\prod_j \mathfrak{a}_j = \prod_{P\in S} P^{\sum_j v_P(\mathfrak{a}_j)} \tag{3}$$

which has valuation 0 for primes Q of $\mathbb{Z}_F, Q \notin S$ and $\mathcal{R}_Q = \mathcal{O}_Q$.

Proof that $\mathcal{R}$ contains $\mathcal{O}$: We have proved above that $\mathcal{R}_Q = \mathcal{O}_Q$ for $Q \notin S$. When $P \in S, \mathcal{R}_P \supseteq \mathcal{O}_P$ follows from the proof below that $\mathcal{R}$ is S-maximal. Therefore $\mathcal{R} = \cap\mathcal{R}_P \supseteq \cap\mathcal{O}_P = \mathcal{O}$. This can also be seen by showing that $d\alpha \in \mathcal{R}$ using that $jv_P(d) \le \mu_{Pj}$ due to minimality of $\mu_{P,j}$ so that $v_P(\mathfrak{a}_j) \le 0$.

Proof that $\mathcal{R}$ is S-maximal: To prove that $\mathcal{R}$ is an S-maximal order we prove that $\mathcal{R}$ is P-maximal for all $P \in S$ by showing that the P-integral basis of Theorem 3.6 is contained in the localization $\mathcal{R}_{P\cap\mathcal{R}}$.

We recall from Theorem 3.6 that $\pi_P^{l_P}(\alpha - z)^{k_P}$, where π_P is a prime element of P, generates a P-integral basis for $\mathcal{O}'_P$ over $\mathcal{O}_P$. We choose π_P such that $v_{\tilde{P}}(\pi_P) \ge 0$ for all $\tilde{P} \in S, \tilde{P} \ne P$. Let $P \in S$, we have

$$\pi_P^{l_P}(\alpha - z)^{k_P} = (1/d)^{k_P}\pi_P^{l_P}(d)^{k_P}(\alpha - z)^{k_P},$$
$$1 = v_P(\pi_P^{l_P}(\alpha - z)^{k_P}) = v_P\left((1/d)^{k_P}\pi_P^{l_P}(d(\alpha - z))^{k_P}\right)$$

therefore $l_P \ge \mu_{P,k_P}$ and

$$\begin{aligned}
&\pi_P^{l_P}(\alpha - z)^{k_P} \\
&= \left(\prod_{Q\in S\setminus P} \pi_Q^{-\mu_{Q,k_P}}\right)\pi_P^{\mu_1}\left(\prod_{Q\in S}\pi_Q^{\mu_{Q,k_P}}\right)(1/d)^{k_P}\omega_{k_P}, \quad \mu_1 = l_P - \mu_{P,k_P} \ge 0 \\
&= \mathfrak{q}\pi_P^{\mu_1}\left(\prod_{Q\in S}\pi_Q^{v_Q(d)}/d\right)^{k_P}\left(\prod_{Q\in S}\pi_Q^{\mu_2}\right)\omega_{k_P}, \quad \mathfrak{q} = \left(\prod_{Q\in S\setminus P}\pi_Q^{-\mu_{Q,k_P}}\right), \mu_2 = \mu_{Q,k_P} - k_P v_Q(d) \\
&= \mathfrak{q}\pi_P^{\mu_1}\left(\prod_{Q\in S}\pi_Q^{v_Q(d)}/d\right)^{k_P} r
\end{aligned}$$

where $r \in \mathcal{R}$ since $(\prod_{Q\in S}\pi_Q^{\mu_2}) \in \mathfrak{a}_{k_P}$.

Therefore $\pi_P^{l_P}(\alpha - z)^{k_P} \in \mathcal{R}_P$ since $\mu_1 \ge 0, v_P(Q) = 0$ and $v_P(\pi_P^{v_P(d)}/d) = 0$ so there is no P in the denominator.

Therefore there is an integral basis of $\mathcal{O}'_P$ over $\mathcal{O}_P$ at each $P \in S$ which is contained in $\mathcal{R}_P$ therefore the integral closure $\mathcal{O}'_P \subseteq \mathcal{R}_P$ but since $\mathcal{R}_P \subseteq \mathcal{O}'_P, \mathcal{R}_P = \mathcal{O}'_P$.

Therefore we have that $v(\text{disc}(\mathcal{R}_{P\cap\mathcal{R}})) = v(\text{disc}(\mathcal{O}'_P))$. Since $\mathcal{O}'_P$ is the localization of $\mathbb{Z}_{F'}$ (the integral closure of $\mathbb{Z}_F$ in F') at P this means that $v_P(\text{disc}(\mathcal{R})) = v_P(\text{disc}(\mathbb{Z}_{F'}))$ by [**PZ89**] p292 (invariance under localization). Therefore $\mathcal{R}$ is P-maximal for all $P \in S$, therefore $\mathcal{R}$ is S-maximal.

□

Proof of Corollary 3.10. Let $\mathcal{R}$ be the module with pseudo basis $(\omega_j, \mathfrak{a}_j)_j$ over $\mathbb{Z}_F$. We know from the second item of the proof of Theorem 3.8 that $\mathcal{R}$ contains only integral elements over $\mathbb{Z}_F$ so it is contained in the integral closure $\mathbb{Z}_{F'}$ of $\mathbb{Z}_F$ in F'/F. We now prove that $\mathbb{Z}_{F'} \subseteq \mathcal{R}$.

Let $\beta \in \mathbb{Z}_{F'}$. Then analogous to [**Mar77**] Theorem 9 and 8,

$$\begin{aligned}\beta &= \sum_{j=0}^{n} b_j (d(\alpha - z))^j / \operatorname{disc}((d(\alpha - z)^j)), \quad \operatorname{disc} \mid b_j^2, b_j \in \mathbb{Z}_F \\ &= 1/(-d)^{p-1} \sum_{j=0}^{n} b_j (d(\alpha - z))^j.\end{aligned}$$

To show that $\beta \in \mathcal{R}$ we need to show that $b_j/(-d)^{p-1} \in \mathfrak{a}_j \, \forall j$, or equivalently $v_P(b_j) \geq \mu_{Pj} + (p-1-j)v_P(d) \, \forall P \in S$. Since $\beta \in \mathbb{Z}_{F'}$ we have $v_{P'}(\beta) \geq 0$ for all $P' \mid P, P \subset \mathbb{Z}_F$. Therefore

$$\begin{aligned}0 &\leq -(p-1)v_{P'}(d) + v_{P'}(\sum_{j=0}^{n} b_j (d(\alpha - z))^j) \\ &= -(p-1)v_{P'}(P)v_P(d) + \min_j \{v_{P'}(b_j) + j v_{P'}(d(\alpha - z))\} \\ 0 &\leq -(p-1)v_{P'}(P)v_P(d) + v_{P'}(b_j) + j v_{P'}(d(\alpha - z)), \forall j \\ &= -(p-1)v_{P'}(P)v_P(d) + v_{P'}(P)v_P(b_j) + j v_{P'}(P)v_P(d) + j v_{P'}((\alpha - z))\end{aligned}$$

and

$$v_P(b_j) \geq (p-1-j)v_P(d) + (-j v_{P'}(\alpha - z)/v_{P'}(P)) > v_P(d)(p-1-j) + \mu_{Pj} - 1$$

so $v_P(b_j) \geq v_P(d)(p-1-j) + \mu_{Pj}, \beta \in \mathcal{R}$ and $\mathbb{Z}_{F'} \subseteq \mathcal{R}$ and hence $\mathcal{R} = \mathbb{Z}_{F'}$. □

3.4. Complexity

We consider the complexity of computing the pseudo basis in Theorem 3.8. Let $v(u) \leq 0$ be the minimum valuation of u for all P (if $v(u) \geq 0$ then $\mathbb{Z}_F[d\alpha]$ is maximal) and $v(d)$ the maximum valuation of $d \, \forall P \in S$. There are p pseudo basis elements

to compute. The powers of $d(\alpha - z)$ cost 1 multiplication for each basis element since they can be computed by repeated multiplication. There are $\#S$ ideals P and $\mu_{P,j} = 0$ when P is unramified and otherwise $\mu_{P,j}$ is at worst $-pv_P(u - \wp(z))/p \leq -v_P(u)$ and also $jv_P(d) \leq pv_P(d)$. To compute $v_P(u)$ is a cost of $O(\log_2(-(v_P(u))))$ multiplications in F. Combined this is a cost of at most $p-1$ multiplications in F', which is $O((p-1)p\log(p)\log(\log(p))) = O(p^2\log(p)\log(\log(p)))$ operations in F, $O(\#S\log_2(-v(u)))$ multiplications in F and $O(\#Sp(\log_2(-v(u) + pv_P(d))))$ ideal multiplications in F. Each number of multiplications is at most linear or linear up to log factors in both the degree of F' and the number of primes and logarithmic in the valuation of the constant coefficient and we have less than $O(p^3)$ operations in F.

To compute each of the $\#S$ z_P we iterate a loop bounded by $v_P(u) \leq v_P(u - \wp(z)) \leq 0$ containing $1 + \log_2(p) + 2\log_2(v(u))$ multiplications in F. However, it is most likely that this loop is iterated only once since there is only a $1/p$ chance that $v(u) \equiv 0 \mod p$. This is a maximum cost of $O(\#S(-v(u))(1+\log_2(p)+2\log_2(-v(u))))$ multiplications in F but this cost could be as low as $O(\#S(1+\log(p)+\log(-v(u))))$ if the loop is iterated only once. To compute z from the z_P we loop another $\#S$ times doing operations in F during strong approximation, however each iteration with $z_P = 0$, a likely case, will be trivial. The number of multiplications here is logarithmic in the degree of the field and the valuation of the constant coefficient and linear in the number of primes to be considered.

Therefore the total complexity as number of operations in F to compute the pseudo basis in Theorem 3.8 is contained in

$$O\left(p^2\log(p)\log(\log(p))\right) + O\left(\#S\log_2(-v(u))\right) + O\left(\#S_r p\log_2(-v(u)+pv(d))\right) + O\left(\#S(-v(u))(\log_2(p)+\log_2(-v(u)))\right)$$

3.5. Examples

We show calculations of maximal orders for a few simple examples using the Theorems in this chapter.

Example 4. *Let $F' = \mathbb{F}_5(t)[x]/\langle x^5 - x - t + 1\rangle, u = t - 1$ and let α be a root of $x^5 - x - t + 1$. Let S be the set of irreducible polynomials in $\mathbb{F}_5[t]$. Then $v_P(u) \geq 0$ for all $P \in S$, so $\mathbb{F}_5[t][\alpha]$ is S-maximal. Now let S be the set of primes $\{1/t\}$ of V_∞, $v_{(1/t)}(u) = -1$ so $1/t$ is ramified*

in F'. We compute $z = 0$ since $m = 1 \not\equiv 0 \mod 5$. We have

$$(\omega_j, \mathfrak{a}_j)_j = \left\{(1,1), \left(\frac{1}{t}\alpha, (\frac{1}{t})^0\right), \left((\frac{1}{t}\alpha)^2, (\frac{1}{t})^{-1}\right), \left((\frac{1}{t}\alpha)^3, (\frac{1}{t})^{-2}\right), \left((\frac{1}{t}\alpha)^4, (\frac{1}{t})^{-3}\right)\right\}$$

since $\mu_{P,j} = \lceil -j(-1)/5 \rceil$ and $d = 1/t$.

Example 5. *Let $F = \mathbb{F}_{11}(t)[x]/\langle x^2+1\rangle$ and let $F' = F[x]/\langle x^{11}-x-t^2+1/t^{11}\rangle, u = t^2-1/t^{11}$ and let α be a root of $x^{11}-x-t^2+1/t^{11}$. Let $S = \mathbb{P}^0_F$. The place $P_t \mid t$ is the only prime in the discriminant of $\mathbb{Z}^0_F[t^{11}\alpha]$, the ideal generated by t^{1210}, at which we have $v_{P_t}(u) = -11$. We compute $v_u = -11 = -1\times 11+0$, take the 11th root of $t^{13}-1 \mod P_t$, set $z = (-1)t^{-1}$ and $u_z = t^2 - 1/t^{11} - ((-1)t^{-11} - (-1)t^{-1}) = t^2 + 1/t$ with $v_u = -1 \not\equiv 0 \mod 11$. We have $d = t^{11}$. So we have*

$$\{(1,1)\} \cup \left\{\left((t^{11}(\alpha + 1/t))^j, t^{1-11j}\right)\right\}_{\{1\le j<11\}},$$

as a pseudo basis for the S-maximal order of $\mathbb{Z}^0_F[t^{11}\alpha]$ since $\mu_{t,j} = \lceil (-j)(-1)/11 \rceil$.

Let $S = \mathbb{P}^\infty_F$. The place $P_{1/t} \mid 1/t$ is the only prime in the discriminant of $\mathbb{Z}^\infty_F[(1/t)\alpha]$, the ideal generated by $(1/t)^{110}$, at which we have $v_{P_{1/t}}(u) = -2 \not\equiv 0 \mod 11$. We have $d = 1/t$. So we have

$$\left\{(1,1), \left(\frac{1}{t}\alpha, (\frac{1}{t})^0\right), \left((\frac{1}{t}\alpha)^2, (\frac{1}{t})^{-1}\right), \left((\frac{1}{t}\alpha)^3, (\frac{1}{t})^{-2}\right), \left((\frac{1}{t}\alpha)^4, (\frac{1}{t})^{-3}\right), \right.$$
$$\left((\frac{1}{t}\alpha)^5, (\frac{1}{t})^{-4}\right), \left((\frac{1}{t}\alpha)^6, (\frac{1}{t})^{-4}\right), \left((\frac{1}{t}\alpha)^7, (\frac{1}{t})^{-5}\right), \left((\frac{1}{t}\alpha)^8, (\frac{1}{t})^{-6}\right),$$
$$\left.\left((\frac{1}{t}\alpha)^9, (\frac{1}{t})^{-7}\right), \left((\frac{1}{t}\alpha)^{10}, (\frac{1}{t})^{-8}\right)\right\}$$

as a pseudo basis for the S-maximal order of $\mathbb{Z}^\infty_F[(1/t)\alpha]$ since $\mu_{1/t,j} = \lceil (-j)(-2)/11 \rceil$.

We give an example over a non-perfect field where we cannot compute a basis.

Example 6. *Let $F = \mathbb{F}_2(a,b,c,d,e)(t)[x]/\langle x^2 + atx + t^3 + (b^2+b)t^2 + c\rangle, \alpha$ a root of $x^2+atx+t^3+(b^2+b)t^2+c$ and $F' = F[x]/\langle x^2+x+d+(t^2+b^2+b)/a^2\rangle, u = d+(t^2+b^2+b)/a^2$. Let P be the prime of F above $1/t$, then $v_P(u) = -4$ and we take the square root of $1/a^2$, set $z = 1/a \times (t/(t^3 + (b^2+b)t^2 + c)\alpha + at^2/(t^3 + (b^2+b)t^2 + c))^{-2}, u = u - (z^2 - z)$ and then we need the square root of $(a+1)/a$ which does not exist in $\mathbb{F}_2(a,b,c,d,e)(t)$. Hence we cannot compute a basis since the constant field of F' is not perfect.*

3.6. A Note on Computing Primes

When comparing the computation of maximal orders using Theorem 3.8 to some other algorithms, it is important to consider how one obtains the primes to use as input. The Round 2 algorithm requires a full factorization of the discriminant of the order which can be expensive and adds to the time taken to compute a maximal order. Both computing a maximal order using Theorem 3.8 and [**Fra05**] require primes but not exponents. [**Fra05**] computes primes using the factorization of the constant coefficient of the defining polynomial of the Artin–Schreier extension. When computing an order maximal at all primes above primes in $\mathbb{P}_F^\infty$ we do the same. But when computing an order maximal at all primes above primes in $\mathbb{P}_F^0$ we compute the discriminant and the primes dividing it without exponents.

The complexity of computing a factorization is relative to the valuations at the prime factors. The valuation of the discriminant at the primes which divide it can be noticeably larger than the valuation of the constant coefficient of the defining polynomial at these primes. To see this let α be a root of $f(x) = x^p - x - u$. The other roots of f are $\alpha + i$ for $i \in \mathbb{F}_p$ ([**Sti93**] Proposition III.7.8). Similarly $d\alpha$ is a root of $x^p - d^{p-1}x - d^p u$ which has roots $d(\alpha + i), i \in \mathbb{F}_p$ so the discriminant is

$$\prod_{0 \le i < j < p} (d(i-j))^2 = d^{2\binom{p}{2}} \prod_{0 \le i < j < p} (i-j)^2,$$

where $\binom{p}{2}$ is a binomial coefficient and evaluates to $p!/((p-2)!2!)$, since the discriminant is the product of the squares of the differences between the roots. But $v_P(d) > 0$ for P such that $v_P(\alpha), v(u) < 0$, in fact, $v_P(d) \ge -v_P(u)$ to ensure $v_P(d\alpha) \ge 0$ so $v_P(d^{2\binom{p}{2}}) \ge -p(p-1)v_P(u)$. Hence computing a factorization of the discriminant will be more expensive than the factorization of the constant coefficient and even more so the larger p is. Computing only the primes dividing the discriminant is also cheaper than the factorization as it avoids any computation of potentially large valuations.

In the results which follow we attempt to split out the time taken to compute the primes which are used.

3.7. Timings

Timings are given for an Intel(R) Core(TM) i7-3770 CPU 3.4GHz (32GB RAM) machine running Magma V2.20-8 under Linux.

In Table 3.1 we compare the times for computing $\mathbb{Z}^0_{F'}$ and $\mathbb{Z}^\infty_{F'}$, the integral closures of $k[t]$ and V_∞ respectively in F', in the examples given above.

		Theorem 3.8		Round 2	
Example	$\#S$	$\mathbb{Z}^0_{F'}$	$\mathbb{Z}^\infty_{F'}$	$\mathbb{Z}^0_{F'}$	$\mathbb{Z}^\infty_{F'}$
1	0, 1	0.0s	0.01s	0.0s	0.01s
2	1, 1	0.04s	0.06s	5.06s	1.71s

TABLE 3.1. Comparison of times for Examples 4 and 5

In Table 3.2 we give a comparison of timings for the computation of $\mathbb{Z}^0_{F'}$ and $\mathbb{Z}^\infty_{F'}$, the integral closures of $k[t]$ and V_∞ respectively in F', for some examples from [**Fra05**] Section 5.2 using Theorem 3.8, Round 2 and [**Fra05**]. All examples are given by $F' = F[y]/\langle y^p - y - u\rangle$ where $F = \mathbb{F}_p(t)[x]/\langle x^3 - (t+1)x^2 + 2xt - t^5\rangle$, ρ is a primitive element of F and $u = \frac{t^5}{t^3-1}\rho^2 + \frac{t^6+t^2+1}{t^6-1}\rho + \frac{1}{t^5}$. Note that Theorem 3.8 and [**Fra05**] may have a considerable advantage over the implementation of the Round 2 in that they do not require the discriminant or its complete factorization, they only require the primes and not the exponents of those primes which can be expensive to compute, especially if large. Once timings became inconveniently large we no longer recorded them. [**Fra05**] reports only times for the computation of finite maximal orders.

We record the maximum time for computing primes (the factorization of the discriminant) in the columns labelled "Primes" and the number of primes occurring in the discriminants in $\#S$. Times given for the Round 2 algorithm do not include the time taken to compute primes, those for Theorem 3.8 and [**Fra05**] do. Note that Theorem 3.8 and [**Fra05**] compute the primes they require more efficiently than the factorization used by Round 2 whose timings are recorded in the "Primes" column.

It is obvious that [**Fra05**] is a considerable improvement on the times for Round 2. We have been able to further improve these times through our implementation which computes maximal orders with pseudo bases stated in Theorem 3.8.

	$\#S$		Primes		Theorem 3.8		[**Fra05**]		Round 2	
p	$\mathbb{P}_F^0$	$\mathbb{P}_F^\infty$	$\mathbb{P}_F^0$	$\mathbb{P}_F^\infty$	$\mathbb{Z}_{F'}^0$	$\mathbb{Z}_{F'}^\infty$	$\mathbb{Z}_{F'}^0$	$\mathbb{Z}_{F'}^\infty$	$\mathbb{Z}_{F'}^0$	$\mathbb{Z}_{F'}^\infty$
5	12	1	0.02s	0.1s	0.07s	0.03s	0.48s	0.41s	3.01s	0.45s
7	15	1	0.05s	0.17s	0.05s	0.05s	0.41s	0.32s	9.13s	0.6s
11	11	1	0.15s	0.83s	0.07s	0.1s	0.52s	0.34s	46.8s	4.41s
23	11	1	1.14s	7.03s	0.4s	0.68s	2.86s	7.18s	1165.91s	88.42s
31	17	1	3.4s	17.76s	0.9s	1.5s	4.39s	50s	73min	240.78s
53	11	1	11.23s	98.92s	3.81s	6.77s	50.25s	319.34s	13hrs	36mins
61	17	1	22s	129.55s	5.98s	9.95s	29.56s	95.19s	$>$ 20hrs	62mins
71	13	1	29.21s	191.81s	9.78s	15.41s	51.84s	268.42s	-	1.9hrs
83	12	1	42.99s	339.26s	15.98s	24.31s	160.92s	1682.6s	-	3.6hrs
97	17	1	81.61s	451.99s	26.77s	38.79s	33min	191.3s	-	6.8hrs

Table 3.2. Comparison of times for examples from [**Fra05**]

Chapter 4

A Note on Decomposing Primes

For both Artin–Schreier extensions and Kummer extensions F'/F we can compute directly an element of valuation 1 at a place $P' \subset F', P' \mid P, P \subset F$ when $P' \mid P$ is totally ramified (Theorem 2.2 and Theorem 3.6). This allows us to decompose easily a prime P which totally ramifies in a Kummer or Artin–Schreier extension as we can construct the prime above P from this known generator in F' and the generators of P which lie in F.

When F'/F is a Kummer extension then P totally ramifies in F' if $v_P(u)$ is coprime to n. When F'/F is an Artin–Schreier extension then P totally ramifies in F' if $v_P(u) < 0$ and there exists $z \in F$ such that $p \nmid v_P(u - (z^p - z)) < 0$. Therefore it is easy to recognise primes of F which ramify in these extensions F'.

Once we have determined that P totally ramifies in F' we can compute an element β with valuation 1 at $P' \mid P$ as we did when computing P-integral bases. When F'/F is a Kummer extension $\beta = \alpha^l \pi^j$ where $1 = lv_P(u) + jn$ (Theorem 2.2, [**Sti93**] Proposition III.7.3). When F'/F is an Artin–Schreier extension $\beta = (\alpha - z_P)^l \pi^j$ where $1 = lv_P(u - (z_P^p - z)) + jp$ adjusted so that $0 \leq l < p$ (Theorem 3.6, [**Sti93**] Proposition III.7.8).

Let $\mathbb{Z}_{F'}$ be the integral closure in F' of $k[t]$ if $k[t] \cap P \neq k$ otherwise of V_∞. Unfortunately β may not be an integral element of F', that is, β may not be in $\mathbb{Z}_{F'}$ which we need for a generator of an integral ideal of $\mathbb{Z}_{F'}$, but we can adjust β to gain such an element. We summarise our approach in the following algorithm.

Algorithm 6 (Decompose a prime which totally ramifies in a Kummer or Artin–Schreier extension)**.**

Input:

- *A cyclic extension F'/F which is either Kummer or Artin–Schreier and a prime $P \subset F$ such that P totally ramifies in F'.*

Output:

- *An element of valuation 1 at $P' \mid P$ which lies in the integral closure of $k[t]$ in F' if $k[t] \cap P \neq k$ otherwise the integral closure of V_∞ in F'.*

Steps:

1. (a) *if F'/F is a Kummer extension set $\beta = \alpha^l \pi^j$ where $1 = lv_P(u) + jn$.*
   (b) *if F'/F is an Artin–Schreier extension set $\beta = (\alpha - z_P)^l \pi^j$ where $1 = lv_P(u - (z^p - z)) + jp$.*
2. *Compute $\delta_\beta = \operatorname{lcm}\{\operatorname{den}(a_i/a_j) \mid 0 \leq i < j < m, a_i, a_j \neq 0\} \in F$, where a_i are the coefficients of the minimal polynomial of β over F of degree $m(= n, p)$ and* den *is the denominator with respect to the integral closure $\mathbb{Z}_F \subset \mathbb{Z}_{F'}$ such that $\mathbb{Z}_F \cap P \neq k$, as in* [**Fra05**] *Proposition 4.1.5,* $\operatorname{den}() : F \to \mathbb{Z}_F \cap k(t)$.
3. *Compute $\gamma \in F$ such that $v_P(\gamma) = -v_P(\delta_\beta)$ and $v_Q(\gamma) \geq 0$ for $Q \subset \mathbb{Z}_{F'}$ using strong approximation.*
4. *Return the product $\gamma\delta_\beta\beta$.*

Theorem 4.1. *Let F'/F be a Kummer or Artin–Schreier extension, P a place of F which totally ramifies in F', $\mathbb{Z}_{F'}$ the integral closure of $k[t]$ or V_∞ in F' such that $P \cap \mathbb{Z}_{F'} \neq k$ and $P' \mid P$. The element $\gamma\delta_\beta\beta$ computed in Algorithm 6 has valuation 1 at P' and is integral at all other primes $Q \subset \mathbb{Z}_{F'}$.*

Proof. We have $v_{P'}(\gamma\delta_\beta\beta) = -v_{P'}(\delta_\beta) + v_{P'}(\delta_\beta) + 1 = 1$ and $v_Q(\gamma\delta_\beta\beta) \geq 0 - v_Q(\beta) + v_Q(\beta) = 0$ so $\gamma\delta_\beta\beta$ is an integral element with valuation 1 at P'. □

Now we can write $P' = P\mathbb{Z}_{F'} + \gamma\delta_\beta\beta\mathbb{Z}_{F'}$. But P may have 2 generators itself so we have possibly 3 generators for P'. If P is principal, which is always the case when F is a rational (function) field or when $P \cap V_\infty \neq k$, then we do have 2 generators for P'. We can also use the generator of $P_K = K \cap P$, where K is the rational (function) field contained in F, and $\gamma\delta_\beta\beta$ as 2 generators for P' if $v_{P_K}(\operatorname{norm}_{F'/K}(\gamma\delta_\beta\beta)) = 1$ ([**Coh93**] Lemma 4.7.9). Note that if P' happens to be a principal ideal then $\gamma\delta_\beta\beta$ is a principal ideal generator for P' only when it has zero valuation at all other primes $Q \subset \mathbb{Z}_{F'}$.

We found that reducing the generator we calculated modulo the generator of P_K improved the efficiency of subsequent calculations with the ideal P'.

Chapter 5

Artin–Schreier–Witt Extensions

Let F be a function field of characteristic $p > 0$ with perfect constant field and $\bar{F}$ the separable closure of F in some algebraic closure. Recall from Definition 1.5 that $W_n(F)$ is the ring of Witt vectors of length n with entries in F. Let $\wp : W_n(\bar{F}) \to W_n(\bar{F})$ be the Artin–Schreier operator $\wp : (x_1, \ldots, x_n) \mapsto (x_1^p, \ldots, x_n^p) - (x_1, \ldots, x_n)$ which is a $\mathrm{Gal}(\bar{F}, F)$-linear and surjective homomorphism ([**Fra05**], Proposition 3.2.3). That $W_n(F)$ has characteristic p^n follows from $px = (0, x_1^p, x_2^p, \ldots)$ ([**Fra05**] Section 1.4) which can be deduced from the secondary components $x^{(i)}$ of x or the use of the shift operator, $V(x_1, x_2, \ldots) = (0, x_1, x_2, \ldots)$ in [**Has80**] page 159–160, for which we have $(p^m x)_i \equiv (V^m x^{p^m})_i \mod p$ and so if $i \leq m, (p^m x)_i = 0$.

Definition 5.1. *An* Artin–Schreier–Witt extension *of F is an abelian extension $E \subseteq \bar{F}$ of F of degree p^n.*

In particular we consider those extensions E/F such that $\mathrm{Gal}(E/F)$ is cyclic for which we have further information.

Theorem 5.2 ([**Fra05**], Theorem 3.2.6)**.** *The following statements are equivalent:*

1. *E/F is a cyclic Artin–Schreier–Witt extension of degree p^n.*
2. *$E = F(\alpha) = F(\wp^{-1}(u))$ where $u = (u_1, \ldots, u_n) \in W_n(F)$ with $\wp(\alpha) = u$ and $u_1 \neq \alpha^p - \alpha$ for all $\alpha \in F$.*

As in [**Fra05**], we consider a cyclic Artin–Schreier–Witt extension E/F of degree p^n with $E = F(\alpha_1, \ldots, \alpha_n), \wp(\alpha) = u$. Set $E_i := F(\alpha_1, \ldots, \alpha_i), 1 \leq i < n$. Then $E_0 := F, E_1, \ldots, E_i$ are the only intermediate fields of E_i/F since E_i/F is cyclic and therefore $E_i = F(\alpha_i)$ and in particular $E = F(\alpha_n)$.

Remark 5.3 ([**Fra05**], Remark 3.2.7)**.** *From Proposition 1.6 we get the recursions*

$$\begin{aligned} u_1 &= \alpha_1^p - \alpha_1, \\ u_2 &= \alpha_2^p - \alpha_2 - z_1, \\ &\vdots \\ u_n &= \alpha_n^p - \alpha_n - z_{n-1} \end{aligned}$$

where $z_i \in E_i$ are polynomial expressions with coefficients in the prime field of F given by $z_0 = 0$ and

$$\begin{aligned} z_i &= -\frac{\alpha_i^{p^2} - \alpha_i^p - u_i^p}{p} - \frac{\alpha_{i-1}^{p^3} - \alpha_{i-1}^{p^2} - u_{i-1}^{p^2}}{p^2} - \ldots - \frac{\alpha_1^{p^{i+1}} - \alpha_1^{p^i} - u_1^{p^i}}{p^i} \\ &= -\frac{(\alpha_i + u_i + z_{i-1})^p - \alpha_i^p - u_i^p}{p} \\ &\qquad - \frac{(\alpha_{i-1} + u_{i-1} + z_{i-2})^{p^2} - \alpha_{i-1}^{p^2} - u_{i-1}^{p^2}}{p^2} - \ldots \\ &\qquad \ldots - \frac{(\alpha_1 + u_1)^{p^i} - \alpha_1^{p^i} - u_1^{p^i}}{p^i}. \end{aligned}$$

Definition 5.4 ([**Fra05**] Section 3.2)**.** *An* Artin–Schreier–Witt generator *of an Artin–Schreier–Witt extension E/F is an element $\alpha = (\alpha_1, \ldots, \alpha_n) \in \wp^{-1}(W_n(F))$ such that $E = F(\alpha_1, \ldots, \alpha_n)$.*

Proposition 5.5 ([**Fra05**] Proposition 3.2.8)**.** *Let E/F be a cyclic Artin–Schreier–Witt extension of degree p^n, i.e. we have $u \in W_n(F), u_1 \neq \alpha^p - \alpha \ \forall \alpha \in F, \alpha = (\alpha_1, \ldots, \alpha_n) \in \wp^{-1}(u)$ and $E = F(\alpha) = F(\alpha_1, \ldots, \alpha_n)$. Then, for $\alpha' \in W_n(\bar{F})$, the following assertions are equivalent:*

1. *α' is an Artin–Schreier–Witt generator of E/F.*
2. *$\alpha' \in \wp^{-1}(u')$ for some $u' \in W_n(F)$ and $u' - \lambda u \in \wp(W_n(F))$ for some $\lambda \in (\mathbb{Z}/p^n\mathbb{Z})^*$.*
3. *$\alpha' = \lambda\alpha + \zeta$ for some $\lambda \in (\mathbb{Z}/p^n\mathbb{Z})^*$ and $\zeta \in W_n(F)$.*

The automorphisms of E/F are given by $\alpha \mapsto \alpha + \zeta, \zeta \in W_n(\mathbb{F}_p) \cong \mathbb{Z}/p^n\mathbb{Z}$ since $\alpha_i \mapsto \alpha_i + \lambda_i, 1 \leq i \leq n, 0 \leq \lambda_i < p$ are the automorphisms of E_i/E_{i-1} and the isomorphism follows from [**Fra05**] Proposition 1.4.5.

Further when E/F is a cyclic Artin–Schreier–Witt extension with intermediate fields E_j as described following Theorem 5.2 we have,

Remark 5.6 (adapted from [**Fra05**] Remark 4.3.1)**.** *Let P_j an arbitrary extension of P to E_j. Since the E_j $(0 \leq j < n)$ are the only subfields of E, we know from Theorem 1.1 that the inertia field of P_n over P is E_t for some $0 \leq t \leq n$, i.e. P is unramified in E_t/F and P_j is totally ramified in E_l/E_j for each $t \leq j < l \leq n$. We claim that*

$$t = \begin{cases} n, & \text{if } \Lambda_{P,i} = 0 \text{ for all } 1 \leq i \leq n \\ \min\{0 \leq i < n | \Lambda_{P,i+1} < 0\}, & \text{otherwise} \end{cases} \tag{4}$$

where $\Lambda_{P,i}$ is described in Algorithm 7.

For a proof of similar to (4) see [**Fra05**] p. 60.

5.1. Artin–Schreier–Witt Quotients

Analogous to Definition 3.2 we can define Artin–Schreier–Witt quotients modulo a prime or a set of primes.

Definition 5.7. *Let $P \in \mathbb{P}_F$ and $u \in W_n(F)$. An* Artin–Schreier–Witt quotient *of u modulo P is an element $\zeta_P \in W_n(F)$ satisfying $v_P((u - \wp(\zeta_P))_i) \geq 0$ or $p \nmid v_P((u - \wp(\zeta_P))_i) < 0$ for all $1 \leq i \leq n$.*

Let $S \subset \mathbb{P}_F$. If ζ is an Artin–Schreier–Witt quotient of u modulo P for all $P \in S$ then we call ζ an Artin–Schreier–Witt quotient *of u modulo S.*

Algorithm 7 (Compute an Artin–Schreier–Witt quotient modulo S ([**Fra05**] Algorithm 4.3.3))**.**

Input:

- *A function field F with perfect constant field, a vector $u \in W_n(F)$ and a set of places $S \subset \mathbb{P}_F$.*

Output:

- *An Artin–Schreier–Witt quotient ζ of u modulo S.*

Steps:

1. *Initialize* $\zeta = (0, \ldots, 0), u' = u, m = 0, \zeta_P = (0, \ldots, 0), \Lambda_P = 0, t_P = n \ \forall P \in S$
2. *while* $m < n$
   (a) *Replace m with $m + 1$*
   (b) *For each $P \in S$ with $\Lambda_P = 0$ do*
      (i) $(\zeta_P)_m, \Lambda_P = \text{ArtinSchreierQuotient}(u'_m, P)$ *(Algorithm 3)*
      (ii) *if $\Lambda_P \neq 0$, set $t_P = m - 1$.*

(c) *Compute ζ_m using strong approximation (*[**Fra05**] *Algorithm 1.3.3) or the extension of the chinese remainder theorem (Algorithm 4) such that $v_P(\zeta_m - (\zeta_P)_m) \geq 1, P \in S$ and $v_Q(\zeta_m) \geq 0$ for $Q \notin S \cup \{X\}$, for some $X \notin S$.*

(d) *Replace u' with $u' - \wp(Z)$ where $Z \in W_n(F)$ is given by*

$$Z_j = \begin{cases} \zeta_m, & j = m \\ 0, & \text{otherwise} \end{cases}$$

3. *Return $\zeta, [(\Lambda_P, t_P)]_{P \in S}$.*

Note that the entries of these Artin–Schreier–Witt quotients ζ are each Artin–Schreier quotients and so we have $p \nmid v_P((u - \wp(\zeta))_i) < 0$ precisely when $i > t$.

5.2. A local P-integral Power Basis

Theorem 5.8. *Let $E = F(\alpha) = F(\wp^{-1}(u))$ be a cyclic Artin–Schreier–Witt extension of degree p^n with perfect constant field. Let P be a place of F, ζ_P an Artin–Schreier–Witt quotient of u modulo P and ρ_P an Artin–Schreier quotient of $u_n + z_{n-1}$ modulo $\{P_{n-1} : (P_{n-1} \mid P)\} \subset \mathbb{P}_{E_{n-1}}$. Let $P' \mid P, P' \in \mathbb{P}_E$.*

When $P' \mid P$ has ramification degree p set

$$B = \{(\alpha - \zeta_P)_1^{i_1} \dots (\alpha - \zeta_P)_{n-1}^{i_{n-1}}((\alpha - \zeta_P)_n^{l_P} \pi_P^{s_P})^j\}_{0 \leq i_1, \dots, i_{n-1} < p, 0 \leq j < p}$$

where $ps_P + v_P((u - \wp(\zeta_P))_n) l_P = 1$. Otherwise set

$$B = \{(\alpha - \zeta_P)_1^{i_1} \dots (\alpha - \zeta_P)_t^{i_t}((\alpha_n - \rho_P)^{l_P} \pi_P^{s_P})^j\}_{0 \leq i_1, \dots i_t < p, 0 \leq j < p^{n-t}}$$

where $p^{n-t} s_P + v_{P_{n-1}}(u_n + z_{n-1} - \wp(\rho_P)) l_P = 1$ and π_P is a uniformizing element of P. Then B is a P-integral basis for E/F.

Proof. By Remark 5.6 there is some t such that $P_t \mid P$ is unramified and $P' \mid P_t$ is totally ramified. Therefore we consider bases $B_u = \{(\alpha - \zeta_P)_1^{i_1} \dots (\alpha - \zeta_P)_t^{i_t}\}_{0 \leq i_1, \dots, i_t < p}$ and $B_r = \{((\alpha_n - \rho_P)^{l_P} \pi_P^{s_P})^j\}_{0 \leq j < p^{n-t}}$ for E_t/F and E/E_t respectively. Taking products of elements of these bases we have $B = \{xy : x \in B_u, y \in B_r\}$.

Since $P_t \mid P$ is unramified, $(\alpha - \zeta_P)_l$ is a root of $\Phi(x) = x^p - x - z'_{l-1} - u'_l$ for which we have $v_{P'}(\Phi'((\alpha - \zeta_P)_l)) = v_{P'}(-1) = 0$ so $\{(\alpha - \zeta_P)_l^i\}_{0 \leq i < p}$ is a P-integral basis for E_l/E_{l-1} by [**Sti93**] Corollary III.5.11 once we prove by induction that z'_j are integral at P where the z'_j correspond to the tower in Remark 5.3 for $u' = u - \wp(\zeta_P)$ and $\alpha' = \alpha - \zeta_P$.

We have $v_P(z'_0) = v_P(0) > 0$. Suppose $v_{P_j}(z'_i) > 0, i < j, P_j \in \mathbb{P}_{E_j}, P_j \mid P$ unramified.

$$
\begin{aligned}
v_{P_j}(z'_j) &= v_{P_j}(-\frac{\alpha_j'^{p^2} - \alpha_j'^{p} - u_j'^{p}}{p} - \frac{\alpha_{j-1}'^{p^3} - \alpha_{j-1}'^{p^2} - u_{j-1}'^{p^2}}{p^2} - \cdots - \frac{\alpha_1'^{p^{j+1}} - \alpha_1'^{p^j} - u_1'^{p^j}}{p^j}) \\
&\geq \min\{v_{P_j}(\frac{\alpha_j'^{p^2} - \alpha_j'^{p} - u_j'^{p}}{p}), v_{P_j}(\frac{\alpha_{j-1}'^{p^3} - \alpha_{j-1}'^{p^2} - u_{j-1}'^{p^2}}{p^2}), \ldots, v_{P_j}(\frac{\alpha_1'^{p^{j+1}} - \alpha_1'^{p^j} - u_1'^{p^j}}{p^j})\} \\
&= \min\{v_{P_j}(\alpha_j'^{p^2} - \alpha_j'^{p} - u_j'^{p}) - v_{P_j}(p), v_{P_j}(\alpha_{j-1}'^{p^3} - \alpha_{j-1}'^{p^2} - u_{j-1}'^{p^2}) - v_{P_j}(p^2), \ldots, \\
&\qquad\qquad v_{P_j}(\alpha_1'^{p^{j+1}} - \alpha_1'^{p^j} - u_1'^{p^j}) - v_{P_j}(p^j))\} \\
&= \min\{v_{P_j}(\alpha_j'^{p^2} - \alpha_j'^{p} - u_j'^{p}), v_{P_j}(\alpha_{j-1}'^{p^3} - \alpha_{j-1}'^{p^2} - u_{j-1}'^{p^2}), \ldots, v_{P_j}(\alpha_1'^{p^{j+1}} - \alpha_1'^{p^j} - u_1'^{p^j})\} \\
&\geq \min\{v_{P_j}(\alpha_j'^{p^2}), v_{P_j}(\alpha_j'^{p}), v_{P_j}(u_j'^{p}), v_{P_j}(\alpha_{j-1}'^{p^3}), v_{P_j}(\alpha_{j-1}'^{p^2}), v_{P_j}(u_{j-1}'^{p^2}), \ldots, \\
&\qquad\qquad v_{P_j}(\alpha_1'^{p^{j+1}}), v_{P_j}(\alpha_1'^{p^j}), v_{P_j}(u_1'^{p^j})\} \\
&= \min\{p^2 v_{P_j}(\alpha'_j), p v_{P_j}(\alpha'_j), p v_{P_j}(u'_j), p^3 v_{P_j}(\alpha'_{j-1}), p^2 v_{P_j}(\alpha'_{j-1}), p^2 v_{P_j}(u_{j-1}), \ldots, \\
&\qquad\qquad p^{j+1} v_{P_j}(\alpha'_1), p^j v_{P_j}(\alpha'_1), p^j v_{P_j}(u'_1)\} \qquad \text{(A)}
\end{aligned}
$$

By Algorithm 3 we have $v_P(u'_i) \geq 0$ when $i \leq j, P_j \mid P$ is unramified so we also have $v_{P_j}(u'_i) \geq 0, i \leq j$. From Remark 5.3 we have $\alpha_i'^{p} - \alpha'_i = u'_i + z'_{i-1}$ so $v_{P_j}(\alpha_i'^{p} - \alpha'_i) = v_{P_j}(u'_i + z'_{i-1}) \geq \min\{v_{P_j}(u'_i), v_{P_j}(z'_{i-1}\} \geq 0, i \leq j$ using the induction hypothesis. But

$$v_{P_j}(u'_i + z'_{i-1}) = v_{P_j}(\alpha_i'^{p} - \alpha'_i) \geq \min\{p v_{P_j}(\alpha'_i), v_{P_j}(\alpha'_i)\}.$$

Suppose $v_{P_j}(\alpha'_i) < 0$. Then $v_{P_j}(u'_i + z'_{i-1}) = p v_{P_j}(\alpha'_i) < 0$ which is a contradiction so $v_{P_j}(\alpha'_i) \geq 0$. Therefore all elements in (A) are non-negative so we must have $v_{P_j}(z'_j) \geq 0$ for $P_j \mid P$ unramified and substituting $j = l - 1$ we have $v_P(z'_{l-1}) > 0$ when $P_{l-1} \mid P$ is unramified. So z'_{l-1} is integral at P, $(\alpha - \zeta_P)_l$ generates a P-integral basis for E_l/E_{l-1} and B_u is a P-integral basis for E_t/F since it is a product of P-integral bases.

Since $P' \mid P_t$ is totally ramified

$$
\begin{aligned}
v_{P'}(\pi_P^{s_P}(\alpha_n - \rho_P)^{l_P}) &= s_P p^n + l_P v_{P'}(\alpha_n - \rho_P) \\
&= s_P p^n + l_P 1/p v_{P'}(u_n + z_{n-1} - \wp(\rho_P)) \\
&= s_P p^n + l_P (1/p) p v_{P_{n-1}}(u_n + z_{n-1} - \wp(\rho_P)) \\
&= 1
\end{aligned}
$$

so B_r is a P-integral basis by [**Sti93**] Proposition III.5.12. Therefore B is a P-integral basis for E/F.

When $P' \mid P$ has ramification degree p, $B_u = \{(\alpha-\zeta_P)_1^{i_1} \dots (\alpha-\zeta_P)_{n-1}^{i_{n-1}}\}$ is a P-integral basis for E_{n-1}/F. To see that $B_r = \{((\alpha-\zeta_P)_n^{l_P}\pi_P^{s_P})^j\}$ is a P-integral basis for E_n/E_{n-1} by [**Sti93**] Proposition III.5.12 note that $\alpha-\zeta_P$ is an Artin–Schreier–Witt generator for E/F and $\alpha-\zeta_P \in \wp^{-1}(u-\wp(\zeta_P))$ by Proposition 5.5. Then similarly to the ramified case,

$$\begin{aligned} v_{P'}((\alpha-\zeta_P)_n^{l_P}\pi_P^{s_P}) &= s_P p + l_P v_{P'}((\alpha-\zeta_P)_n) \\ &= s_P p + l_P 1/p v_{P'}((u-\wp(\zeta_P))_n + z'_{n-1}) \\ &= s_P p + l_P (1/p) p v_{P_{n-1}}((u-\wp(\zeta_P))_n + z'_{n-1}) \\ &= s_p p + l_P v_{P_{n-1}}((u-\wp(\zeta_P))_n) \\ &= 1 \end{aligned}$$

since $v_{P_{n-1}}(z'_{n-1}) \geq 0$ as $P_{n-1} \mid P$ is unramified and $v_{P_{n-1}}((u-\wp(\zeta_P))_n) < 0$ so $v_{P_{n-1}}((u-\wp(\zeta_P))_n) \neq v_{P_{n-1}}(z'_{n-1})$ and

$$v_{P_{n-1}}((u-\wp(\zeta_P))_n + z'_{n-1}) = v_{P_{n-1}}((u-\wp(\zeta_P))_n) = v_P((u-\wp(\zeta_P))_n).$$

Therefore B is a P-integral basis for E/F. □

Comparing to Theorem 1.1 we see that in an Artin–Schreier–Witt extension the decomposition of the place $P \subset F$ is determined by the valuation of the entries of u at P. The place P splits in $E_i \subset Z$, the decomposition field of E/F, when $v_P(u_i) > 0$. We have that $P_i \mid P_Z$ is inert in E_i/Z and $p \mid v_P(u_i) < 0, v_P((u-\wp(\zeta))_i) \geq 0$ for $t_Z < i \leq t$ where $E_{t_Z} = Z$.

5.3. Computing S-Maximal Modules

In this section we will again assume that E/F is a cyclic Artin–Schreier–Witt extension, $E = F(\alpha) = F(\wp^{-1}(u))$ with perfect constant field. We work towards computing a maximal order of E. We leave the computation of S-maximal orders until Section 5.6 as the proofs are longer and computing a maximal order is more interesting. We instead make statements about S-maximal modules (Definition 1.4) which are easier to prove and sufficient to compute a maximal order.

We start with an order $\mathcal{O} = \mathbb{Z}_F[d\alpha_n]$ where $\mathbb{Z}_F$ is the integral closure of $k[t]$ or V_∞ in F, $d \in \mathbb{Z}_F \cap k(t)$ and $v_{P'}(d\alpha_n) \geq 0$ for all $P' \mid P$, P a prime ideal of $\mathbb{Z}_F$. We also need $d_l \in \mathbb{Z}_F \cap k(t)$ such that $v_{P_l}(d_l\alpha_l) \geq 0$ for all $P_l \mid P$, P a prime ideal of $\mathbb{Z}_F$ and $P_l \subset E_l$.

Theorem 5.9. *Let $E = F(\alpha) = F(\wp^{-1}(u))$ be an Artin–Schreier–Witt extension of degree p^n and S a set of primes of $\mathbb{Z}_F$ with the same ramification degree p^{n-t}. Let $\zeta \in F$ be an*

Artin–Schreier–Witt quotient of u modulo S computed using Algorithm 7. Let $\rho \in E_{n-1}$ be an Artin–Schreier quotient of $u_n + z_{n-1}$ modulo $\{P' : P' \mid P, P \in S \mid e(P'|P) > p\}$ such that $v_Q(\rho) \geq 0$ for all $Q \notin \{P' : P' \mid P, P \in S \mid e(P'|P) > p\} \cup \{X\}$ for some place X such that $X \cap \mathbb{Z}_F = k$. Let d_l be such that $v_{P_l}(d_l\alpha_l) \geq 0$ for all $P_l \mid P$, P a prime ideal of $\mathbb{Z}_F$ and let $v_{P,ij} = jv_P(d) + \sum_{l=1}^{t} i_l v_P(d_l)$. Then

$$(\omega_{ij}, \mathfrak{a}_{ij})_{ij} = ((d_1(\alpha-\zeta)_1)^{i_1} \dots (d_t(\alpha-\zeta)_t)^{i_t}(d(\alpha_n-\rho))^j, \prod_{P\in S} P^{\mu_{P,j}-v_{P,ij}})_{0\leq i_1,\dots,i_t<p, 0\leq j<p^{n-t}}$$

or, more efficiently when the ramification index $p^{n-t} = p$,

$$(\omega_{ij}, \mathfrak{a}_{ij})_{ij} = ((d_1(\alpha-\zeta)_1)^{i_1} \dots (d_{n-1}(\alpha-\zeta)_{n-1})^{i_{n-1}}(d(\alpha-\zeta)_n)^j, \prod_{P\in S} P^{\mu_{P,j}-v_{P,ij}})_{0\leq i_1,\dots,i_{n-1}<p, 0\leq j<p}$$

is a pseudo basis for an integral module of E over $\mathbb{Z}_F$ which is S-maximal where $\mu_{P,j}$ is the smallest non-negative integer such that $v_{P'}(\mathfrak{a}_{ij}\omega_{ij}) \geq 0$ for all $P' \mid P \in S$ and all i.

To compute $\mu_{P,j}$, let $P' \mid P$. We require $v_{P'}((\alpha-\zeta_1)^{i_1} \dots (\alpha-\zeta)_t^{i_t}(\alpha_n-\rho)^j P^{\mu_{P,j}}) \geq 0$ since all the d and d_l valuations cancel, that is, $i_1 v_{P'}((\alpha-\zeta)_1) + \dots + i_t v_{P'}((\alpha-\zeta)_t) + jv_{P'}(\alpha_n-\rho) + \mu_{P,j}v_{P'}(P) \geq 0$. For each $P \in S$ we can add $1 + \pi_P$ to $(\zeta_P)_l$ (Chapter 3 following the proof of Theorem 3.6) before completing Algorithm 3 called from Algorithm 7 to ensure that $v_{P'}((\alpha-\zeta)_l) \leq 1$ if it isn't already. Therefore we need

$$\mu_{P,j} \geq \frac{-jv_{P'}(\alpha_n-\rho))}{p^{n-t}} = \frac{-jv_{P_{n-1}}(u_n+z_{n-1}-\wp(\rho))}{p^{n-t}},$$

where $P_{n-1} \mid P, P_{n-1} \subset E_{n-1}$, so we take

$$\mu_{P,j} = \left\lceil \frac{-jv_{P_{n-1}}(u_n+z_{n-1}-\wp(\rho))}{p^{n-t}} \right\rceil$$

and similarly

$$\mu_{Pj} = \left\lceil \frac{-jv_P((u-\wp(\zeta))_n)}{p} \right\rceil$$

when the ramification degree of P in E is p.

Note that ζ and ρ can be quotients for sets S where the places may have different ramification degrees. We compute such elements using strong approximation or chinese remainder with all primes (or all primes contained in E_{n-1} above) the primes in S.

Remark 5.10. *Let $\mathcal{R}$ be the module with pseudo basis $(\omega_{ij}, \mathfrak{a}_{ij})_{ij}$ over $\mathbb{Z}_F$. Note that the index of $\mathcal{O}$ in $\mathcal{R}$ does not contain only primes in S. This index will be the determinant of the transformation matrix $\{\omega_{ij}\}$ multiplied by the coefficient ideals $\mathfrak{a}_{ij}$. The product*

of the coefficient ideals obviously contains only primes in S but the determinant of the transformation matrix may contain other primes. This is what prevents $\mathcal{R}$ being an S-maximal over order of $\mathcal{O}$ although we do prove that $\mathcal{R}$ is an order in Theorem 5.16. As shown in the proof below of Theorem 5.17 the exponents in the coefficient ideals are all non-positive.

Proof of Theorem 5.9. Let $\mathcal{R}$ be the module with pseudo basis $(\omega_{ij}, \mathfrak{a}_{ij})_{ij}$ over $\mathbb{Z}_F$. We prove that $\mathcal{R}$ contains elements integral over $\mathbb{Z}_F$ so $\mathcal{R}$ is contained in the integral closure $\mathbb{Z}_E$ of $\mathbb{Z}_F$ in E and that $\mathcal{R}$ is S-maximal.

Proof that $\mathcal{R}$ is an integral module over $\mathbb{Z}_F$: We constructed $(\omega_{ij}, \mathfrak{a}_{ij})_{ij}$ such that $v_{P'}(\mathfrak{a}_{ij}\omega_{ij}) \geq 0$ for all $P' \mid P, P \in S$. Let Q be a prime of E lying above a prime of $\mathbb{Z}_F$ which is not in S. We chose the exceptional place for the strong approximation which computed each ζ_l to be a prime not contained in $\mathbb{Z}_F$ so we assume Q does not lie above the exceptional prime. We have

$$v_Q(\mathfrak{a}_{ij}\omega_{ij}) = \sum_{P\in S} v_Q(P)(\mu_{Pj} - jv_P(d) - \sum_{l=1}^{t} i_l v_P(d_l)) + \sum_{l=1}^{t}(i_l v_Q(d_l(\alpha-\zeta)_l)) + jv_Q(d(\alpha_n - \rho))$$

$$= \sum_{l=1}^{t} i_l v_Q(d_l(\alpha-\zeta)_l) + j(v_Q(d) + v_Q(\alpha_n - \rho))$$

or

$$v_Q(\mathfrak{a}_{ij}\omega_{ij}) = \sum_{l=1}^{n-1} i_l v_Q(d_l(\alpha-\zeta)_l) + j(v_Q((\alpha-\zeta)_n) + v_Q(d))$$

when the ramification index is p.

Since $v_Q(\rho) \geq 0$ by construction of ρ, $v_Q(\alpha_n - \rho) \geq \min\{v_Q(\alpha_n), v_Q(\rho)\}$, $0 \leq v_Q(d\alpha_n)$ and $v_Q(d) \geq 0$ we either have

$$v_Q(\mathfrak{a}_{ij}\omega_{ij}) \geq \sum_{l=1}^{t} i_l v_Q(d_l(\alpha-\zeta)_l) + j(v_Q(d) + v_Q(\rho)) \geq \sum_{l=1}^{t} i_l v_Q(d_l(\alpha-\zeta)_l)$$

or

$$v_Q(\mathfrak{a}_{ij}\omega_{ij}) \geq \sum_{l=1}^{t} i_l v_Q(d_l(\alpha-\zeta)_l) + j(v_Q(d) + v_Q(\alpha_n)) \geq \sum_{l=1}^{t} i_l v_Q(d_l(\alpha-\zeta)_l).$$

When the ramification index is p, $(\alpha-\zeta)_n = \alpha_n - \eta$ for some $\eta \in F, v_Q(\eta) \geq 0$ by construction using strong approximation, so $v_Q((\alpha-\zeta)_n) \geq \min\{v_Q(\alpha_n), v_Q(\eta)\}$ and

$$v_Q(\mathfrak{a}_{ij}\omega_{ij}) \geq \sum_{l=1}^{n-1} i_l v_Q(d_l(\alpha-\zeta)_l) + j(v_Q(\alpha_n) + v_Q(d)) \geq \sum_{l=1}^{n-1} i_l v_Q(d_l(\alpha-\zeta)_l)$$

or

$$v_Q(\mathfrak{a}_{ij}\omega_{ij}) \geq \sum_{l=1}^{n-1} i_l v_Q(d_l(\alpha-\zeta)_l) + j(v_Q(\eta) + v_Q(d)) \geq \sum_{l=1}^{n-1} i_l v_Q(d_l(\alpha-\zeta)_l).$$

The result follows in all cases on proving $v_Q(d_l(\alpha-\zeta)_l) \geq 0$. But we have $(\alpha-\zeta)_l = \alpha_l - \eta_l$ for some $\eta_l \in F, v_Q(\eta_l) \geq 0$ by construction using strong approximation, so $v_Q((\alpha-\zeta)_l) \geq \min\{v_Q(\alpha_l), v_Q(\eta_l)\}$ and

$$\begin{aligned} v_Q(d_l(\alpha-\zeta)_l) &\geq \begin{cases} v_Q(d_l) + v_Q(\alpha_l), & v_Q(\alpha_l) \leq v_Q(\eta_l) \\ v_Q(d_l) + v_Q(\eta_l), & \text{otherwise} \end{cases} \\ &\geq 0 \end{aligned}$$

since $v_Q(d_l) \geq 0, v_Q(\eta_l) \geq 0$ and $v_Q(d_l\alpha_l) \geq 0$.

Proof that $\mathcal{R}$ is S-maximal : To prove that $\mathcal{R}$ is an S-maximal module we prove that $\mathcal{R}$ is P-maximal for all $P \in S$ by showing that the P-integral basis of Theorem 5.8 is contained in the localization $\mathcal{R}_{P\cap\mathcal{R}}$ of $\mathcal{R}$ at P.

We recall from Theorem 5.8 that $(\alpha-\zeta)_1, \ldots, (\alpha-\zeta)_t$ and $\pi_P^{s_P}(\alpha-\zeta)_n^{l_P}$ or $\pi_P^{s_P}(\alpha_n-\rho)^{l_P}$, where π_P is a prime element of P, generate a P-integral basis for $\mathcal{O}'_P$ over $\mathcal{O}_P$. We choose π_P such that $v_{\tilde{P}}(\pi_P) \geq 0$ for all $\tilde{P} \in S, \tilde{P} \neq P$. Let $P \in S$, we have

$$\pi_P^{s_P}(\alpha-\zeta)_n^{l_P} = (\frac{1}{d})^{l_P}\pi_P^{s_P}(d)^{l_P}(\alpha-\zeta)_n^{l_P},$$

$$1 = v_P(\pi_P^{s_P}(\alpha-\zeta)_n^{l_P}) = v_P\left((\frac{1}{d})^{l_P}\pi_P^{s_P}(d)^{l_P}(\alpha-\zeta)_n^{l_P}\right),$$

$$\pi_P^{s_P}(\alpha_n-\rho)^{l_P} = (\frac{1}{d})^{l_P}\pi_P^{s_P}(d)^{l_P}(\alpha_n-\rho)^{l_P},$$

$$1 = v_P(\pi_P^{s_P}(\alpha_n-\rho)^{l_P}) = v_P\left((\frac{1}{d})^{l_P}\pi_P^{s_P}(d)^{l_P}(\alpha_n-\rho)_n^{l_P}\right).$$

Therefore in both cases $s_P \geq \mu_{P,l_P}$ by minimality of μ_{P,l_P} and

$$(\alpha-\zeta)_l = \frac{1}{d_l}\omega_{0\dots1\dots00} = \left(\frac{\prod_{Q\in S}\pi_Q^{v_Q(d_l)}}{d_l}\right)(\prod_{Q\in S}\pi^{-v_Q(d_l)})\omega_{0\dots1\dots00}$$
$$= \left(\frac{\prod_{Q\in S}\pi_Q^{v_Q(d_l)}}{d_l}\right) r.$$

Also

$$\pi_P^{s_P}(\alpha-\zeta)_n^{l_P} = (\prod_{Q\in S\setminus P}\pi_Q^{-\mu_{Ql_P}})\pi_P^{\mu_1}(\prod_{Q\in S}\pi_Q^{\mu_{Ql_P}})(\frac{1}{d})^{l_P}\omega_{0l_P}, \quad \mu_1 = s_P - \mu_{Pl_P} \geq 0,$$

$$\pi_P^{s_P}(\alpha_n-\rho)^{l_P} = (\prod_{Q\in S\setminus P}\pi_Q^{-\mu_{Ql_P}})\pi_P^{\mu_1}(\prod_{Q\in S}\pi_Q^{\mu_{Ql_P}})(\frac{1}{d})^{l_P}\omega_{0l_P}, \quad \mu_1 = s_P - \mu_{Pl_P} \geq 0$$
$$= (\prod_{Q\in S\setminus P}\pi_Q^{-\mu_{Ql_P}})\pi_P^{\mu_1}\left(\frac{\prod_{Q\in S}\pi_Q^{v_Q(d)}}{d}\right)^{l_P}(\prod_{Q\in S}\pi_Q^{\mu_2})\omega_{0l_P},\ \mu_2 = \mu_{Ql_P} - l_P v_Q(d)$$
$$= (\prod_{Q\in S\setminus P}\pi_Q^{-\mu_{Ql_P}})\pi_P^{\mu_1}\left(\frac{\prod_{Q\in S}\pi_Q^{v_Q(d)}}{d}\right)^{l_P} r$$

where $r \in \mathcal{R}$ since $(\prod_{Q\in S}\pi^{-v_Q(d_l)}) \in \mathfrak{a}_{0\dots1\dots00}$ for all l and $(\prod_{Q\in S}\pi_Q^{\mu_2}) \in \mathfrak{a}_{il_P}$ for all i. Therefore $(\alpha-\zeta)_1,\dots,(\alpha-\zeta)_t$ and $\pi_P^{s_P}(\alpha-\zeta)_n^{l_P}$ or $\pi_P^{s_P}(\alpha_n-\rho)^{l_P}$ are in the localization $\mathcal{R}_P$ since $s_P - \mu_{Pl_P} \geq 0, v_P(Q) = 0, Q \in S\setminus\{P\}$ and $v_P(\pi_P^{v_P(d_l)}/d_l) = v_P(\pi_P^{v_P(d)}/d) = 0$ so there is no P in the denominator.

Therefore there is an integral basis of $\mathcal{O}'_P$ over $\mathcal{O}_P$ at each $P \in S$ which is contained in the localization $\mathcal{R}_P$ so the integral closure $\mathcal{O}'_P$ is contained in the localization $\mathcal{R}_P$ but since $\mathcal{R}_P \subseteq \mathcal{O}'_P$, $\mathcal{R}_P = \mathcal{O}'_P$. Therefore we have that $v(\mathrm{disc}(\mathcal{R}_P)) = v(\mathrm{disc}(\mathcal{O}'_P))$. Since $\mathcal{O}'_P$ is the localization of $\mathbb{Z}_{F'}$ (the integral closure of $\mathbb{Z}_F$ in F') at P this means that $v_P(\mathrm{disc}(\mathcal{R})) = v_P(\mathrm{disc}(\mathbb{Z}_{F'}))$ by [**PZ89**] p292 (invariance under localization). Therefore $\mathcal{R}$ is P-maximal for all $P \in S$, therefore $\mathcal{R}$ is S-maximal.

□

Remark 5.11. *When S contains only primes of ramification degree greater than p we have $d\alpha_n = d(\alpha_n-\rho) + d\rho = \omega_{01} + d\rho$. We have $v_{P'}(P^{\mu_{P,j}}(\alpha_n-\rho)^j) \geq 0$ by definition of $\mu_{P,j}$.*

We also have

$$\begin{aligned} v_{P'}(P^{jv_P(d)}(\alpha_n-\rho)^j) &= j(v_{P'}(d)+v_{P'}(\alpha_n-\rho)) \\ &\geq j(v_{P'}(d)+v_{P'}(\alpha_n)) \\ &= jv_{P'}(d\alpha_n) \\ &\geq 0 \end{aligned}$$

so $jv_P(d) \geq \mu_{P,j}$ *by minimality of* $\mu_{P,j}$ *Therefore* $1 \in \mathfrak{a}_{01}$. *Since* $v_{P'}(\rho) \geq v_{P'}(\alpha_n)$ *we have* $v_{P'}(d\rho) \geq v_{P'}(d\alpha_n) \geq 0$ *but* $\mathcal{R}$ *is sometimes too small so that* $d\rho \notin \mathcal{R}$.

We also have $d_l\alpha_l = d_l(\alpha-\zeta)_l + d_l\eta_l$ *when* $l \leq t$ *so as above we have* $\mathbb{Z}_F[d_l\alpha_l] \subseteq \mathcal{R}$.

For a set $S \subset \mathbb{P}_F$ which may contain places of differing ramification degrees we join the pseudo bases for each subset $S_l \subset S$ containing primes of S having ramification degree p^l and reduce it using normal form. This is equivalent to addition of modules.

Algorithm 8 (Compute an S-maximal integral module in an Artin–Schreier–Witt Extension)**.**

Input:

- *An Artin–Schreier–Witt extension* $E/F = F(\alpha) = F(\wp^{-1}(u)), u \in W_n(F)$ *of characteristic* p *and degree* p^n *and a set* S *of primes of the integral closure* $\mathbb{Z}_F$ *of* $k[t]$ *or* V_∞ *in* F.

Output:

- *An integral module of* E *over* $\mathbb{Z}_F$ *which is* S*-maximal.*

Steps:

1. *Compute an Artin–Schreier–Witt quotient* ζ *of* u *mod* S *(Algorithm 7) and partition the primes in* S *into sets* S_l *containing primes of ramification degree* p^l.
2. *Compute an Artin–Schreier quotient* ρ *of* $u_n + z_{n-1} \mod \bigcup_{l>1} S_l$ *(Algorithm 5), using Strong Approximation (*[**Fra05**] *Algorithm 1.3.3) or the extension of the Chinese remainder theorem (Algorithm 4) to compute* ρ *from* ρ_P *for primes of all ramification degrees* $> p$. *(One Strong Approximation or Chinese Remainder with all primes is better so that the module resulting is more likely to be an order.)*
3. *For each ramification degree* $p^l, 0 \leq l \leq n$
   (a) *Compute the pseudo basis using unramified generators* $(\alpha-\zeta)_i, 1 \leq i \leq n-l$ *and ramified generator* $(\alpha_n-\rho)$ *stated in Theorem 5.9.*
4. *Return the sum of the modules defined by these pseudo bases.*

Remark 5.12. *The module computed using Algorithm 8 contains $\mathcal{O} = \mathbb{Z}_F[d\alpha_n]$ when S contains a prime with ramification degree p or 1. This follows from Theorem 5.17.*

Theorem 5.13. *The module computed using Algorithm 8 is S-maximal.*

Proof. Let $\mathcal{R} = \sum_{\{l:\#S_l>0\}} \mathcal{R}_l$ be the output of Algorithm 8 where we sum only over those l for which S_l is not empty. Each module $\mathcal{R}_l$ is S_l-maximal. The module $\mathcal{R} = \sum_{\{l:\#S_l>0\}} \mathcal{R}_l$ contains each $\mathcal{R}_l$ and so must be S_l-maximal for each l. Therefore $\mathcal{R}$ is S-maximal. □

5.4. Computing Integral Closures

Algorithm 9 (Compute a maximal order in an Artin–Schreier–Witt extension)**.**
Input:

- *An Artin–Schreier–Witt extension $E/F = F(\alpha) = F(\wp^{-1}(u)), u \in W_n(F)$ of characteristic p and degree p^n and an integral closure $\mathbb{Z}_F$ of $k[t]$ or V_∞ in F.*

Output:

- *The integral closure of $\mathbb{Z}_F$ in E.*

Steps:

1. *Compute the set S of primes in the Witt vector u which occur with negative exponent.*
2. *Compute an S-maximal integral module $\mathcal{S}$ of E/F using Algorithm 8.*
3. *If $S_0 \subset S$ or $S_1 \subset S$ is not empty then return $\mathcal{S}$.*
4. *Otherwise, compute the discriminant of $\mathcal{S}$ (which should be smaller that of $\mathbb{Z}_F[d\alpha_n]$), factorise the minimum and decompose these factors in F to compute the set of primes S_0 $\mathcal{S}$ is not maximal at. These primes will be unramified and since they do not appear in u with negative exponent they will have Artin-Schreier–Witt quotient 0. If S_0 is not empty compute the module $\mathcal{S}_0$ with pseudo basis using unramified generators $d_i\alpha_i$ using Algorithm 8.*
5. *Return the sum of the modules $\mathcal{S}$ and $\mathcal{S}_0$.*

If S_0 is not empty then $\mathcal{R}_0 \subseteq \mathcal{S}$. If S_1 is not empty then $\mathcal{S}_0 \subseteq \mathcal{R}_1 \subseteq \mathcal{S}$ since the ω_{ij} are the same for these ramification degrees and $jv_P(d) - \mu_{P,j} \leq 0$ as in the proof of Theorem 5.17 and Remark 5.11. In both these cases we can avoid the potentially expensive discriminant calculation in Step 4 because we have already calculated pseudo bases at primes of ramification degree 1 and p.

Theorem 5.14. *The module computed using Algorithm 9 is the integral closure of $\mathbb{Z}_F$ in E.*

Proof. Let $\mathcal{R} = \sum_{\{l:\#S_l>0\}} \mathcal{R}_l$ be the output of Algorithm 9 where we sum only over l such that S_l is not empty. Since $\mathcal{R}$ contains each $\mathcal{R}_l$ which is S_l-maximal $\mathcal{R}$ is S_l-maximal for all l. Since each $\mathcal{R}_l$ contains only elements integral over $\mathbb{Z}_F$, $\mathcal{R}$ contains only elements integral over $\mathbb{Z}_F$. Therefore $\mathcal{R}$ is a maximal integral module of E over $\mathbb{Z}_F$. But the maximal order of E containing $\mathbb{Z}_F$ is also a maximal integral module of E. Therefore $\mathcal{R}$ is the maximal order of E containing $\mathbb{Z}_F$ or equivalently the integral closure of $\mathbb{Z}_F$ in E.

□

5.5. A Note on Complexity

The complexity of Algorithms 8, 9 and 10 is not necessarily linear in the degree of the field like the algorithms described in Chapters 2 and 3 due to the use of a normal form algorithm to add together the modules computed from primes of different ramification degrees. The complexity of Algorithms 8 and 9 depends on the number of different ramification degrees places in S have in E. These algorithms are most efficient when S contains only primes of ramification degree p or less and a normal form computation may not be necessary.

It is possible to reduce the number of generators for the sum of the modules by noticing that some of the ω_{ij} are common between differing ramification degrees. For such matching ω_{ij} the final $\mathfrak{a}_{ij}$ is the product of the $\mathfrak{a}_{ij}$ over the different ramification degrees. This smaller input to the normal form algorithm makes the normal form computation cheaper. To do this matching we divide our primes into 2 groups, those with ramification degree $\leq p$ and those with ramification degree $> p$.

The cost of Algorithms 8, 9 and 10 includes the cost of computing the pseudo basis in Theorem 5.9. We now consider the complexity of computing the pseudo basis in Theorem 5.9. To compute $d_l(\alpha-\zeta)_l^{i_l}$ for $0 \leq i_l < p$ takes $p-1$ multiplications in E and to compute $d(\alpha_n-\rho)^j$ for $0 \leq j < p^{n-t}$ takes $p^{n-t}-1$ multiplications in E or one multiplication for each of p^n-1 elements. We compute p^n powers of $\#S$ ideals bounded in exponent (in absolute value) by $-v_P((u-\wp(u))_n)+n(p-1)\max_{P\in S}\{v_P(d)\}$ or $-v_{P_{n-1}}(u_n+z_{n-1}-\wp(\rho))+n(p-1)\max_{P\in S}\{v_P(d)\}$. Computing ζ costs $O(\#Sn(-v(u))(\log_2(p)+\log_2(-v(u)))+\log(p)n^4\log(n)\log(\log(n)))$ in the computation of the quotients and the Witt vector arithmetic. To compute ρ requires $\#S_r(1+\log_2(p)+2\log_2(v(u_n)))$ multiplications in E_{n-1} where S_r is the subset of S containing ideals with ramification degree >1 in

E_{n-1}. The cost of computing $v_P(u_i)$ is $\log_2(v_P(u_i))$ and we require this computation for n entries u_i and $\#S$ ideals P, that is, we compute $n\#S$ valuations. Similarly to Section 3.4 we have an estimated cost in

$$O(p^{2n}n\log(p)\log(n\log(p))) + O(\#S\log_2(-v(u))) + O(\#Sp^n\log_2(-v(u)+npv(d)))+ \\ O(\#S(-v(u))n(\log_2(p)+\log_2(-v(u))) + \log(p)n^4\log(n)\log(\log(n)))$$

to compute the pseudo basis in Theorem 5.9.

However in practice, as can be seen in the timings which follow, Algorithm 9 is faster than Round 2 [**Coh00**] and in some cases much faster. For a range of fields Algorithm 9 is faster than computing a maximal order of the representation of the extension as a tower of n extensions of degree p (similar to an implementation of [**Fra05**] but using Chapter 3 to compute maximal orders of the degree p extensions) and transferring this order across to the degree p^n extension.

5.6. Computing S-Maximal Orders

Here we provide an algorithm for computing the S-maximal over order of the order $\mathbb{Z}_F[d\alpha_n]$ in an Artin–Schreier–Witt extension. We prove this algorithm is correct and also prove that the S-maximal module with basis given in Theorem 5.9 is also an order.

Algorithm 10. *(Compute the S-maximal over order of the order $\mathbb{Z}_F[d\alpha_n]$ in an Artin–Schreier–Witt extension)*

Input:

- *An order $\mathbb{Z}_F[d\alpha_n]$ of an Artin–Schreier–Witt extension $E/F = F(\alpha) = F(\wp^{-1}(u))$, $u \in W_n(F)$ of characteristic p, where $d \in \mathbb{Z}_F \cap k(t)$, and degree p^n and a set S of primes of the integral closure $\mathbb{Z}_F$ of $k[t]$ or V_∞ in F.*

Output:

- *The S-maximal over order of $\mathbb{Z}_F[d\alpha_n]$ over $\mathbb{Z}_F$.*

Steps:

1. *Compute an S-maximal integral module $\mathcal{S}$ using Algorithm 8.*
2. *Return the module sum $b\mathcal{S}+\mathbb{Z}_F[d\alpha_n]$ where $b = \operatorname{disc}(\mathbb{Z}_F[d\alpha_n])/c$ and c is the product of powers of those primes in S which divide $\operatorname{disc}(\mathbb{Z}_F[d\alpha_n])$ such that b is coprime to c and the primes in S* [**Fie13a**].

Theorem 5.15. *The module computed using Algorithm 10 is the S-maximal over order of $\mathbb{Z}_F[d\alpha_n]$.*

Proof. Let $\mathcal{R} = b\mathcal{S} + \mathbb{Z}_F[d\alpha_n]$ be the module computed using Algorithm 10 and let $\mathbb{Z}_E$ be the integral closure of $\mathbb{Z}_F$ in E. We have $\mathcal{R} \supset \mathbb{Z}_F[d\alpha_n]$ and $\mathcal{R}$ is an integral module as it is the sum of integral modules.

We also have $(\mathcal{R})_P \supset (b\mathcal{S})_P = (\mathcal{S})_P = (\mathbb{Z}_E)_P \forall P \in S$ since $\mathcal{S}$ is S-maximal and $v_P(b) = 0$. Therefore $\mathcal{R}$ is contained in $\mathbb{Z}_E$ and contains the S-maximal order of $\mathbb{Z}_F[d\alpha_n]$.

We now prove that $\mathcal{R}$ is no larger than the S-maximal over order of $\mathbb{Z}_F[d\alpha_n]$. If $\mathcal{R}$ is not the S-maximal over order of $\mathbb{Z}_F[d\alpha_n]$ then the index of $\mathbb{Z}_F[d\alpha_n]$ in $\mathcal{R}$ will have non-zero valuation at primes other than those in S. We show that this is not the case. We have

$$\mathbb{Z}_F^{p^n} \supseteq c\mathcal{R} \supseteq c\mathbb{Z}_F^{p^n}$$

and $[Z_F^{p^n} : c\mathbb{Z}_F^{p^n}] = c^{p^n}$. But $[\mathbb{Z}_F^{p^n} : c\mathcal{R}] = \det(c\mathcal{R})$ so $\det(c\mathcal{R})|c^{p^n}$. We also have $[\mathcal{R} : \mathbb{Z}_F[d\alpha_n]] = \det(\mathcal{R}) = \det(c\mathcal{R})/c^{p^n}$ which has valuation 0 at primes not in S. Therefore $\mathcal{R}$ is the S-maximal over order of $\mathbb{Z}_F[d\alpha_n]$. □

Theorem 5.16. *The S-maximal module with pseudo basis given in Theorem 5.9 is an S-maximal order.*

Proof. Let

$$\mathcal{R} = \bigoplus_{(i_1,\ldots,i_t,j)=(0,\ldots,0,0)}^{(p-1,\ldots,p-1,p^{n-t}-1)} \mathfrak{a}_{(i_1,\ldots,i_t)j}\omega_{(i_1,\ldots,i_t)j}$$

be the module of E with pseudo basis $(\omega_{ij}, \mathfrak{a}_{ij})_{ij}$ over $\mathbb{Z}_F$. For $i = j = 0, \omega_{00} = 1, \mu_{P,j} = 0$ so $\mathfrak{a}_{ij} = 1$ and $1 \in \mathcal{R}$.

To prove that $\mathcal{R}$ is closed under multiplication we check that $\mathfrak{a}_{ij}\omega_{ij} \times \mathfrak{a}_{lm}\omega_{lm} \subset \mathcal{R}$. We know that $\mathfrak{a}_{i_100\ldots00}\omega_{i_100\ldots00} \times \mathfrak{a}_{0i_20\ldots00}\omega_{0i_20\ldots00} = \mathfrak{a}_{i_1i_20\ldots00}\omega_{i_1i_20\ldots00} \subset \mathcal{R}$ and similarly so we need to prove $\mathfrak{a}_{i_10\ldots00}\omega_{i_10\ldots00} \times \mathfrak{a}_{i_1'0\ldots00}\omega_{i_1'0\ldots00} \subset \mathcal{R}$ and similarly.

Let i and l be vectors of length t either zero or with one non-zero entry each, ι and κ respectively, in the same position I, $\iota, \kappa \in [0 \ldots p)$ and let $j, m \in [0 \ldots p^{n-t}), j = m = 0$ unless i and l are zero vectors. We have

$$\mathfrak{a}_{ij}\omega_{ij} \times \mathfrak{a}_{lm}\omega_{lm} = \mathfrak{a}_{ij}\mathfrak{a}_{lm}\omega_{ij}\omega_{lm} = \prod_{P\in S} P^{\mu_{P,j}+\mu_{P,m}-v_{P,ij}-v_{P,lm}}\omega_{ij}\omega_{lm}$$

and this pseudo element is integral over all $P \in S$ since $v_{P'}(\mathfrak{a}_{ij}\omega_{ij} \times \mathfrak{a}_{lm}\omega_{lm}) = v_{P'}(\mathfrak{a}_{ij}\omega_{ij}) + v_{P'}(\mathfrak{a}_{lm}\omega_{lm}) \geq 0$ holds for $P' \mid P$. When $\iota + \kappa < p$ or $j + m < p^{n-t}$ this implies $\mu_{P,j} + \mu_{P,m} \geq \mu_{P,(j+m)}$ for all $P \in S$ since $\mu_{P,(j+m)}$ is minimal with this property. So we have

$$\mathfrak{a}_{ij}\omega_{ij} \times \mathfrak{a}_{lm}\omega_{lm} = \prod_{P\in S} P^{\mu}\mathfrak{a}_{(i+l)(j+m)}\omega_{(i+l)(j+m)} \subset \mathcal{R}, \quad \mu = \mu_{P,j} + \mu_{P,m} - \mu_{P,(j+m)}.$$

We now consider 3 cases.

1. When $j = m = 0, \iota + \kappa \geq p$, $\omega_{0\dots(\iota+\kappa)\dots0} = \omega_{0\dots(\iota+\kappa-p)\dots0}\omega_{0\dots p\dots0}$ and

$$\omega_{0\dots p\dots0} = (d_I(\alpha - \zeta)_I)^p = d_I^p(\alpha - \zeta)_I + d_I^p(u'_I + z'_{I-1})$$

so

$$\begin{aligned}\omega_{0\dots(\iota+\kappa)\dots0} &= \omega_{0\dots(\iota+\kappa-p)\dots0}(d_I^{p-1}\omega_{0\dots1\dots0} + d_I^p(u'_I + z'_{I-1})) \\ &= d_I^{p-1}\omega_{0\dots(\iota+\kappa-p+1)\dots0} + d_I^p\omega_{0\dots(\iota+\kappa-p)\dots0}((u - \wp(\zeta))_I + z'_{I-1})\end{aligned}$$

and

$$\text{(B)}\quad \mathfrak{a}_{i0}\omega_{i0} \times \mathfrak{a}_{l0}\omega_{l0} = \prod_{P\in S} P^{\mu}\left(d_I^{p-1}\omega_{0\dots(\iota+\kappa-p+1)\dots0} + d_I^p\omega_{0\dots(\iota+\kappa-p)\dots0}((u - \wp(\zeta))_I + z'_{I-1})\right),$$

where $\mu = \mu_{P,0} + \mu_{P,0} - v_P(d_I)(\iota + \kappa)$. We need to show that the coefficients of

$$\mathfrak{a}_{0\dots(\iota+\kappa-p+1)\dots0}\omega_{0\dots(\iota+\kappa-p+1)\dots0} \text{ and } \mathfrak{a}_{0\dots(\iota+\kappa-p)\dots0}\omega_{0\dots(\iota+\kappa-p)\dots0}$$

in (B) are contained in $\mathbb{Z}_F$. At $P \in S$, since $\mu_{P,0} = 0$,

$$\mathfrak{a}_{0\dots(\iota+\kappa-p+1)\dots0} = \prod_{P\in S} P^{-v_P(d_I)(\iota+\kappa-p+1)}, \mathfrak{a}_{0\dots(\iota+\kappa-p)\dots0} = \prod_{P\in S} P^{-v_P(d_I)(\iota+\kappa-p)}$$

and the coefficient $d_I^{p-1}\prod_{P\in S} P^{-v_P(d_I)(p-1)}$ of $\mathfrak{a}_{0\dots(\iota+\kappa-p+1)\dots0}\omega_{0\dots(\iota+\kappa-p+1)\dots0}$ is integral. The coefficient of $\mathfrak{a}_{0\dots(\iota+\kappa-p)\dots0}\omega_{0\dots(\iota+\kappa-p)\dots0}$ is

$$d_I^p \prod_{P\in S} P^{-pv_P(d_I)}((u - \wp(\zeta))_I + z'_{I-1}).$$

We know from the proof of Theorem 5.8 that z'_{I-1} is integral at $P \in S$ for $I \leq t$ and we also have that $v_P((u - \zeta)_I) \geq 0$ by definition of Artin–Schreier–Witt quotient so both coefficients are integral at $P \in S$. At primes $Q \notin S, Q \subset \mathbb{Z}_F$,

$$\begin{aligned}v_Q(d_I^p \prod_{P\in S} P^{-pv_P(d_I)}((u - \wp(\zeta))_I + z'_{I-1})) &= v_Q(d_I^p((u - \wp(\zeta))_I + z'_{I-1})) \\ &= v_Q((d_I(\alpha - \zeta)_I)^p - d_I^p(\alpha_i - \zeta)_I) \\ &\geq 0\end{aligned}$$

so $d_I^p \prod_{P\in S} P^{-v_P(d_I)}((u-\wp(\zeta))_I + z'_{I-1})$ is integral for all primes Q of $\mathbb{Z}_F$ and

$$\begin{aligned}\mathfrak{a}_{i0}\omega_{i0} \times \mathfrak{a}_{l0}\omega_{l0} = d_I^{p-1} \prod_{P\in S} P^{-v_P(d_I)(p-1)}\mathfrak{a}_{0\dots(\iota+\kappa-p+1)\dots 0}\omega_{0\dots(\iota+\kappa-p+1)\dots 0} + \\ d_I^p \prod_{P\in S} P^{-pv_P(d_I)}((u-\wp(\zeta))_I + z'_{I-1})\mathfrak{a}_{0\dots(\iota+\kappa-p)\dots 0}\omega_{0\dots(\iota+\kappa-p)\dots 0} \\ \subset \mathcal{R}.\end{aligned}$$

2. When the ramification degree of all $P \in S$ in E is p, and $j+m \geq p$ then $\omega_{0(j+m)} = \omega_{0(j+m-p)}\omega_{0p}$ and

$$\omega_{0p} = (d(\alpha-\zeta)_n)^p = d^p((\alpha-\zeta)_n + u'_n + z'_{n-1})$$

so

$$\begin{aligned}&\mathfrak{a}_{0j}\omega_{0j} \times \mathfrak{a}_{0m}\omega_{0m} \\ &= \mathfrak{a}_{0j}\mathfrak{a}_{0m}\omega_{0(j+m-p)}d^p((\alpha-\zeta)_n + u'_n + z'_{n-1}) \\ &= \mathfrak{a}_{0j}\mathfrak{a}_{0m}\omega_{0(j+m-p)}(d^{p-1}\omega_{01} + d^p(u'_n + z'_{n-1})) \\ &= \prod_{P\in S} P^{\mu_{P,j}+\mu_{P,m}-v_P(d)(j+m)}(d^{p-1}\omega_{0(j+m-p+1)} + d^p(u'_n + z'_{n-1})\omega_{0(j+m-p)}) \\ &= \prod_{P\in S} P^{\mu_1} d^{p-1}\mathfrak{a}_{0(j+m-p+1)}\omega_{0(j+m-p+1)} + \\ &\qquad\qquad d^p(u'_n + z'_{n-1}) \prod_{P\in S} P^{\mu_2}\mathfrak{a}_{0(j+l-p)}\omega_{0(j+m-p)},\end{aligned}$$

$$\mu_1 = \mu_{P,j} + \mu_{P,m} - \big(\mu_{P,(j+m-p+1)} - v_P(d)(-p+1)\big)$$

$$\mu_2 = \mu_{P,j} + \mu_{P,m} - \big(\mu_{P,(j+m-p)} - v_P(d)(-p)\big)$$

and we need to prove that

$$\mathfrak{d} = \prod_{P\in S} P^{v_{P\mathfrak{d}}}, \quad v_{P\mathfrak{d}} = \mu_{P,j} + \mu_{P,m} - \mu_{P,(j+m-p+1)}$$

and

$$\mathfrak{c} = d^p(u'_n + z'_{n-1}) \prod_{P\in S} P^{v_{P\mathfrak{c}}}, \quad v_{P\mathfrak{c}} = \mu_{P,j} + \mu_{P,m} - \mu_{P,(j+m-p)} - pv_P(d)$$

are integral at $P \in S$. We have

$$\begin{aligned}&\mathfrak{d}\mathfrak{a}_{0(j+m-p+1)}\omega_{0(j+m-p+1)} \\ &= \prod_{P\in S} P^{\mu}\omega_{0(j+m-p+1)}, \quad \mu = \mu_{P,j} + \mu_{P,m} - v_P(d)(j+m-p+1)\end{aligned}$$

and for $P_n \mid P \in S$, $P_n \subset E$

$$\begin{aligned}
&v_{P_n}(\mathfrak{d}\mathfrak{a}_{0(j+m-p+1)}\omega_{0(j+m-p+1)}) \\
&= p^{n-t}(\mu_{P,j} + \mu_{P,m} - (j+m-p+1)v_P(d)) + (j+m-p+1)v_{P_n}(\omega_{01}) \\
&= p^{n-t}\mu_{P,j} + jv_{P_n}((\alpha-\zeta)_n) + p^{n-t}\mu_{P,m} + mv_{P_n}((\alpha-\zeta)_n) - \\
&\qquad\qquad (1-p)v_{P_n}(d) + (1-p)v_{P_n}(\omega_{01}) \\
&\geq (1-p)v_{P_n}\left((\alpha-\zeta)_n\right)
\end{aligned}$$

by definition of $\mu_{P,j}$ and $\mu_{P,l}$. Since $v_{P_n}((\alpha-\zeta)_n) \leq -1$ and $1-p \leq -1$ we have $v_{P_n}(\mathfrak{d}\mathfrak{a}_{0(j+m-p+1)}\omega_{0(j+m-p+1)}) \geq 1$ and so $\mu_{P,j} + \mu_{P,m} \geq \mu_{P,(j+m-p+1)}$ by minimality of $\mu_{P,(j+m-p+1)}$. Therefore $\mathfrak{d}$ is integral at all $P \in S$.

For the coefficient $\mathfrak{c} = d^p(u'_n + z'_{n-1})\prod_{P\in S} P^{v_{P_\mathfrak{c}}}$ of $\mathfrak{a}_{0(j+m-p)}\omega_{0(j+m-p)}$ we have, for $P_n \mid P \in S$

$$\begin{aligned}
v_{P_n}(\mathfrak{c}) &= pv_{P_{n-1}}(u'_n + z'_{n-1}) + p(\mu_{P,j} + \mu_{P,m} - \mu_{P,(j+m-p)}) \\
&= pv_P((u-\wp(\zeta))_n) + p(\mu_{P,j} + \mu_{P,m} - \mu_{P,(j+m-p)}) \\
&= -p\mu_{P,p} + p(\mu_{P,j} + \mu_{P,m} - \mu_{P,(j+m-p)}) \\
&\geq -p\mu_{P,p} + p\mu_{P,p} \\
&= 0
\end{aligned}$$

since $v_{P_{n-1}}(u'_n + z'_{n-1}) = v_P((u-\wp(\zeta))_n)$ as in the proof of Theorem 5.8 and

$$\begin{aligned}
\mu_{P,(j+m-p)} &= \lceil -(j+m-p)v_P((u-\wp(\zeta))_n)/p \rceil \\
&= \lceil -jv_P((u-\wp(\zeta))_n)/p + -mv_P((u-\wp(\zeta))_n)/p \rceil - -v_P((u-\wp(\zeta))_n) \\
&= \lceil -jv_P((u-\wp(\zeta))_n)/p + -mv_P((u-\wp(\zeta))_n)/p \rceil - \mu_{Pp} \\
&\leq \mu_{P,j} + \mu_{P,m} - \mu_{P,p}.
\end{aligned}$$

Therefore $\mathfrak{c}$ is integral at all $P \in S$. For primes $Q \notin S, Q \subset \mathbb{Z}_F$,

$$v_Q(\mathfrak{c}) = v_Q(d^p(u'_n + z'_{n-1})) = v_Q((d(\alpha-\zeta)_n)^p - d^p(\alpha-\zeta)_n) \geq 0.$$

Therefore

$$\begin{aligned}
&\mathfrak{a}_{0j}\omega_{0j} \times \mathfrak{a}_{0l}\omega_{0l} \\
&= d^{p-1}\prod_{P\in S} P^{-v_P(d)(p-1)}\mathfrak{d}\mathfrak{a}_{0(j+l-p+1)}\omega_{0(j+l-p+1)} + \mathfrak{c}\mathfrak{a}_{0(j+l-p)}\omega_{0(j+l-p)} \\
&\subset \mathcal{R}.
\end{aligned}$$

3. Otherwise, let $j < p^{n-t}, m < p, j+m \geq p^{n-t}$. We have

$$\begin{aligned}\omega_{0p} = (d(\alpha_n - \rho))^p &= d^p(\alpha_n - \rho + u_n + z_{n-1} - \wp(\rho)) \\ &= d^{p-1}\omega_{01} + d^p(u_n + z_{n-1} - \wp(\rho))\end{aligned}$$

therefore

$$\omega_{0j}\omega_{0m} = \omega_{0(j+m-p)}\left(d^p(u_n + z_{n-1} - \wp(\rho)) + d^{p-1}\omega_{01}\right)$$

and

$$\begin{aligned}&\mathfrak{a}_{0j}\omega_{0j} \times \mathfrak{a}_{0m}\omega_{0m} \\ &= \mathfrak{a}_{0j}\mathfrak{a}_{0m}\omega_{0(j+m-p)}\left(d^p(u_n + z_{n-1} - \wp(\rho)) + d^{p-1}\omega_{01}\right) \\ &= (d^{p-1})\prod_{P\in S} P^{\mu}\omega_{0(j+m-p)}\omega_{01} + (d^p)\prod_{P\in S} P^{\mu}\omega_{0(j+m-p)}(u_n + z_{n-1} - \wp(\rho)), \\ &\subset \mathcal{R}\end{aligned}$$

where $\mu = \mu_{P,j} + \mu_{P,m} - v_P(d)(j+m)$ by the argument in 2. above.

We prove that $\mathfrak{a}_{0j}\omega_{0j} \times \mathfrak{a}_{0m}\omega_{0m} \subset \mathcal{R}$ for $m > p$ using induction. Suppose $\mathfrak{a}_{0j}\omega_{0j} \times \mathfrak{a}_{0m}\omega_{0m} \subset \mathcal{R}$ when $m < p^{l-1}, l \leq n-t$. Now let $m < p^l$, then

$$\begin{aligned}&\mathfrak{a}_{0j}\omega_{0j} \times \mathfrak{a}_{0m}\omega_{0m} \\ &= \mathfrak{a}_{0j}\mathfrak{a}_{0m}\omega_{0(j+m-p^l)}\omega_{0p}^{p^{l-1}} \\ &= \mathfrak{a}_{0j}\mathfrak{a}_{0m}\omega_{0(j+m-p^l)}\left((d^{p-1})^{p^{l-1}}\omega_{0p^{l-1}} + d^{p^l}(u_n + z_{n-1} - \wp(\rho))^{p^{l-1}}\right) \\ &= \mathfrak{a}_{0j}\mathfrak{a}_{0m}(d^{p-1})^{p^{l-1}}\omega_{0(j+m-p^l+p^{l-1})} + \mathfrak{a}_{0j}\mathfrak{a}_{0m}d^{p^l}\left(u_n + z_{n-1} - \wp(\rho)\right)^{p^{l-1}}\omega_{0(j+m-p^l)} \\ &= \mathfrak{a}_{0j}\mathfrak{a}_{0m}(d^{p-1})^{p^{l-1}}\omega_{0(j+m-p^l+1)}\omega_{0(p^{l-1}-1)} + \\ &\qquad\qquad \mathfrak{a}_{0j}\mathfrak{a}_{0m}d^{p^l}(u_n + z_{n-1} - \wp(\rho))^{p^{l-1}}\omega_{0(j+m-p^l)}.\end{aligned}$$

Let

$$\mathfrak{c} = d^{p^l}\left(u_n + z_{n-1} - \wp(\rho)\right)^{p^{l-1}}\prod_{P\in S} P^{v_P\mathfrak{c}},$$

where $v_{P\mathfrak{c}} = \mu_{P,j} + \mu_{P,m} - \mu_{P,(j+m-p^l)} - v_P(d)p^l$. To show $\mathfrak{c}$ is integral we have for $P_n \mid P \in S$

$$\begin{aligned}
&v_{P_n}\left(d^{p^l}(u_n + z_{n-1} - \wp(\rho))^{p^{l-1}} \prod_{P\in S} P^{v_{P\mathfrak{c}}}\right)\\
&= pp^{l-1}v_{P_{n-1}}(u_n + z_{n-1} - \wp(\rho)) + p^{n-t}(\mu_{P,j} + \mu_{P,m} - \mu_{P,(j+m-p^l)})\\
&\geq p^l v_{P_{n-1}}(u_n + z_{n-1} - \wp(\rho)) + p^l(\mu_{P,j} + \mu_{P,m} - \mu_{P,(j+m-p^l)})\\
&= -p^l\mu_{Pp^l} + p^l(\mu_{P,j} + \mu_{P,m} - \mu_{P,(j+m-p^l)})\\
&\geq -p^l\mu_{P,p^l} + p^l\mu_{P,p^l}\\
&= 0.
\end{aligned}$$

For primes $Q \notin S, Q \subset \mathbb{Z}_F$,

$$\begin{aligned}
v_Q(\mathfrak{c}) &= v_Q(d^{p^l}(u_n + z_{n-1} - \wp(\rho))^{p^{l-1}})\\
&= p^{l-1}v_Q((d(\alpha_n - \rho))^p - d^p(\alpha_n - \rho))\\
&\geq 0.
\end{aligned}$$

Let $\mathfrak{d} = \prod_{P\in S} P^{v_{P\mathfrak{d}}}, v_{P\mathfrak{d}} = \mu_{P,j} + \mu_{P,m} - (\mu_{P,(j+m-p^l+1)} + \mu_{P,p^l-1})$. To show $\mathfrak{d}$ is integral consider

$$\begin{aligned}
&\mu_{P,(j+m-p^l+1)} + \mu_{P,p^{l-1}-1}\\
&= \lceil -(j+m-p^l+1)v_{P_{n-1}}(u_n + z_{n-1} - \wp(\rho))/p^{n-t}\rceil\\
&\qquad\qquad + \lceil -(p^{l-1}-1)v_{P_{n-1}}(u_n + z_{n-1} - \wp(\rho))/p^{n-t}\rceil\\
&\leq \lceil -((j+m-p^l) + p^{l-1})v_{P_{n-1}}(u_n + z_{n-1} - \wp(\rho))/p^{n-t}\rceil + 2\\
&< \lceil -(j+m-p^{n-t})v_{P_{n-1}}(u_n + z_{n-1} + \wp(\rho))/p^{n-t}\rceil + 2\\
&\leq \mu_{P,j} + \mu_{P,m} + \lceil p^{n-t}v_{P_{n-1}}(u_n + z_{n-1} + \wp(\rho))/p^{n-t}\rceil + 2\\
&= \mu_{P,j} + \mu_{P,m} + \lceil v_{P_{n-1}}(u_n + z_{n-1} + \wp(\rho))\rceil + 2\\
&\leq \mu_{P,j} + \mu_{P,m} - 1 + 2
\end{aligned}$$

since $(j+m-p^l) + p^{l-1} > j+m-p^l \geq j+m-p^{n-t}$. Therefore we have $\mu_{P,(j+m-p^l)} + \mu_{P,p^{l-1}} < \mu_{P,j} + \mu_{P,m} + 1$ so $\mu_{P,(j+m-p^{n-t})} + \mu_{P,p^{n-t-1}} \leq \mu_{P,j} + \mu_{P,m}$ and hence $\mathfrak{d}$ is integral for $P \in S$.

Since $\mathfrak{c}$ and $\mathfrak{d}$ are integral at all primes of $\mathbb{Z}_F$ we have

$$\mathfrak{a}_{0j}\omega_{0j} \times \mathfrak{a}_{0m}\omega_{0m} =$$
$$d^{p^l-p^{l-1}} \prod_{P\in S} P^{-v_P(d)(p^l-p^{l-1})} \mathfrak{d}\mathfrak{a}_{0(j+m-p^l+1)}\omega_{0(j+m-p^l+1)}\mathfrak{a}_{0p^{l-1}-1}\omega_{0p^{l-1}-1} +$$
$$\mathfrak{c}\mathfrak{a}_{0(j+m-p^l)}\omega_{0(j+m-p^l)}$$

and since $\mathfrak{a}_{0(j+m-p^l+1)}\omega_{0(j+m-p^l+1)}\mathfrak{a}_{0p^{l-1}-1}\omega_{0p^{l-1}-1} \subset \mathcal{R}$ by the induction hypothesis $\mathfrak{a}_{0j}\omega_{0j} \times \mathfrak{a}_{0m}\omega_{0m} \subset \mathcal{R}$ for $m < p^l$. Therefore we have proved by induction that $\mathfrak{a}_{0j}\omega_{0j} \times \mathfrak{a}_{0m}\omega_{0m} \subset \mathcal{R}$ for $j, m < p^{n-t}, j + m \geq p^{n-t}$.

□

Theorem 5.17. *In the situation of Theorem 5.9 the module with this pseudo basis contains $\mathcal{O}$ when the primes in S have ramification degree at most p or when $\rho \in F$, including the trivial case when $\rho = 0$, that is $p \nmid v_{P'}(u_n + z_{n-1}) < 0, \forall P' \mid P \in S$.*

Proof of Theorem 5.17. We have $\{(d\alpha_n)^j\}$ as a power basis of the order $\mathcal{O}$. It is enough to prove $d\alpha_n \in \mathcal{R}$. We have $d\alpha_n = d(\alpha_n - \eta) + d\eta = d(\alpha - \zeta)_n + d\eta$ where $\eta \in F$ is such that $(\alpha - \zeta)_n = \alpha_n - \eta$. Therefore $d\alpha_n = \omega_{0\ldots01} + d\eta$. We have $v_P(d) \geq 0$ for all primes P of $\mathbb{Z}_F$ and

$$v_P(\eta) = v_P(\alpha_n - \eta - \alpha_n) \geq \min\{v_P(\alpha_n - \eta), v_P(\alpha_n)\} = \min\{v_P((\alpha - \zeta)_n), v_P(\alpha_n)\} = v_P(\alpha_n)$$

when $v_P(\alpha_n) < 0$ since $v_P((\alpha - \zeta)_n) \geq v_P(\alpha_n)$. Therefore $v_P(d\eta) \geq v_P(d\alpha_n) \geq 0$ so $d\eta \in \mathfrak{a}_{00} = 1$. We also have $\mathfrak{a}_{0\ldots010} = 1$ and $1 \in \mathfrak{a}_{0\ldots01}$, since

$$v_{P'}(P^{jv_P(d)}(\alpha - \zeta)_n^j) = p^{n-t} j v_P(d) + j v_{P'}(\alpha - \zeta)_n \geq j v_{P'}(d) + j v_{P'}(\alpha_n) = j v_{P'}(d\alpha_n) \geq 0$$

so $jv_P(d) \geq \mu_{Pj}$ by minimality of $\mu_{P,j}$ so $d\alpha_n \in \mathcal{R}$ and $\mathcal{O} \subseteq \mathcal{R}$.

When $\rho = 0, d\alpha_n = \omega_{01}$ and $1 \in \mathfrak{a}_{01}$ as in Remark 5.11 so $d\alpha_n \in \mathcal{R}$ and $\mathcal{O} \subseteq \mathcal{R}$. When $\rho \in F, d\alpha_n = d(\alpha_n - \rho) + d\rho = \omega_{01} + d\rho$. We have

$$v_P(\rho) = v_P(\alpha_n - \rho - \alpha_n) \geq \min\{v_P(\alpha_n - \rho), v_P(\alpha_n)\} = v_P(\alpha_n),$$

so $v_P(d\rho) \geq v_P(d\alpha_n) \geq 0$ so $d\rho \in \mathfrak{a}_{00} = 1, d\alpha_n \in \mathcal{R}$ and $\mathcal{O} \subset \mathcal{R}$. □

Note that Theorem 5.17 does not hold when $\rho \notin F$, see Remark 5.11.

5.7. Examples

We provide some examples of calculations of pseudo bases for integral closures of $k[t]$ in Artin–Schreier–Witt extensions of a function field F. In these examples we give as much information as can comfortably fit, we leave out specifying elements which take up a lot of space. Where modules are stated to be orders they have been verified by Magma to be so. We give the discriminants of the S-maximal orders computed by Algorithm 8 rather than those of the S-maximal over orders of $\mathbb{Z}_F^0[d\alpha]$ computed using Algorithm 10, where $\mathbb{Z}_F^0$ is the integral closure of $k[t]$ in F, as these discriminants are often closer to that of the integral closure $\mathbb{Z}_E^0$ of $k[t]$ in E which we ultimately compute.

Example 7. *Let* $F = \mathbb{F}_2(t), u = (1/t^2, 1/(t^2+t))$ *and* $S = \{(t), (t+1)\}$. *Then*

$$E = F(\wp^{-1}(u)) = F(\alpha) = F(\beta)(\gamma) = F(\gamma)$$

where β *is a root of* $x^2 + x + 1/t^2$ *and* γ *is a root of* $x^2 + x + 1/t^2\beta + 1/(t^2+t)$ *over* $F(\beta)$ *and*

$$x^4 + (t^{10} + t^6)x^2 + (t^{13} + t^{12} + t^{11} + t^{10})x + t^{15} + t^{14} + t^{13} + t^{10}$$

over F. *The place* (t) *totally ramifies in* E *and the place* $(t+1)$ *has ramification degree* $p = 2$. *We have* $d_1 = t$ *so* $t\beta$ *is integral and* $d = (t+1)t^3$ *so* $(t^4 + t^3)\gamma$ *is integral. The discriminant of* $\mathbb{F}_2[t][d\gamma]$ *is* $t^{28}(t+1)^{12}$.

We compute an Artin–Schreier–Witt quotient $\zeta = (1/t, 0)$ *and an Artin–Schreier quotient* $\rho_{(t)} = (1/t)\beta + 1/t^2 \mod (t)$ *and* $\rho = (t)^{-2}(t\beta+1)$ *by strong approximation. Therefore*

$$(\omega_{ij}, \mathfrak{a}_{ij})_{ij} = \{(1,1), (d(\alpha-\zeta)_2, (t+1)^0), (d_1(\alpha-\zeta)_1, 1), (d_1(\alpha-\zeta)_1 d(\alpha-\zeta)_2, (t+1)^0)\}$$

is a pseudo basis for a $(t+1)$*-maximal order since* $\mu_{(t+1)j} = \lceil -j(-1)/2 \rceil, v_{(t+1)}(d) = 1$ *and*

$$(\omega_{ij}, \mathfrak{a}_{ij})_{ij} = \{(1,1), (d(\gamma-\rho), t^{-2}), (d^2(\gamma-\rho)^2, t^{-4}), (d^3(\gamma-\rho)^3, t^{-6})\}$$

is a pseudo basis for a (t)*-maximal order since* $\mu_{(t)j} = \lceil -j(-3)/4 \rceil, v_{(t)}(d) = 3$. *The discriminant of the* $(t+1)$*-maximal order described by the first pseudo basis above is* $t^{24}(t+1)^4$, *the discriminant of the* (t)*-maximal order described by the second pseudo basis above is* $t^8(t+1)^{12}$ *and the discriminant of the* $\{(t), (t+1)\}$*-maximal order generated by the concatenation of the two pseudo bases, which is also the integral closure* $\mathbb{Z}_E^0$ *of* $k[t]$ *in* E, *is* $t^8(t+1)^4$.

Example 8. *Let* $F = \mathbb{F}_5(t)[x]/\langle x^2+t^3+t+1\rangle, u = (1/(t^2+3)\lambda+t^2, 1/(t+4)\lambda+t)$ *where* λ *is a root of* x^2+t^3+t+1 *(*[**Fra05**] *Example 19) and let* $S = \{(t+4),(t^2+3)\}$. *Then*

$$E = F(\wp^{-1}(u)) = F(\alpha) = F(\beta)(\gamma) = F(\gamma)$$

where β *is a root of* $x^5-x+4/(t^2+3)\lambda+4t^2$ *and* γ *is a root of* $x^5-x-\upsilon$ *for some* $\upsilon \in F(\beta)$ *over* $F(\beta)$ *and also a root of a degree 25 polynomial over* F. *The place* (t^2+3) *totally ramifies in* E *and the place* $(t+4)$ *has ramification degree* $p = 5$. *We have* $d_1 = t^2+3$ *so* $(t^2+3)\beta$ *is integral and* $d = (t+4)(t^2+3)^5$ *so* $(t^{11}+4t^{10}+3t+2)\gamma$ *is integral. The discriminant of* $\mathbb{Z}_F[d\gamma]$ *is divisible by* $(t+4)^{600}(t^2+3)^{2600}$.

We compute an Artin–Schreier–Witt quotient $\zeta = (0,0)$ *and an Artin–Schreier quotient* $\rho_{(t^2+3)} = 0$ *so* $\rho = 0$. *Therefore*

$$(\omega_{ij},\mathfrak{a}_{ij}) = \{((d_1\beta)^i,1),((d_1\beta)^i(d\gamma),1),((d_1\beta)^i(d\gamma)^2,(t+4)^{-1}),$$
$$((d_1\beta)^i(d\gamma)^3,(t+4)^{-2}),((d_1\beta)^i(d\gamma)^4,(t+4)^{-3})\}_{0\le i<5}$$

is a pseudo basis for a $(t+4)$*-maximal order since* $\mu_{(t+4)j} = \lceil -j(-1)/5\rceil, v_{(t+4)}(d) = 1$ *and*

$$(\omega_{ij},\mathfrak{a}_{ij}) = \{(1,1),(d\gamma,(t^2+3)^{-4}),((d\gamma)^2,(t^2+3)^{-8}),((d\gamma)^3,(t^2+3)^{-12},((d\gamma)^4,(t^2+3)^{-16}),$$
$$((d\gamma)^5,(t^2+3)^{-20}),((d\gamma)^6,(t^2+3)^{-24}),((d\gamma)^7,(t^2+3)^{-29}),((d\gamma)^8,(t^2+3)^{-33}),$$
$$((d\gamma)^9,(t^2+3)^{-37}),((d\gamma)^{10},(t^2+3)^{-41}),((d\gamma)^{11},(t^2+3)^{-45}),((d\gamma)^{12},(t^2+3)^{-49}),$$
$$((d\gamma)^{13},(t^2+3)^{-54}),((d\gamma)^{14},(t^2+3)^{-58}),((d\gamma)^{15},(t^2+3)^{-62}),((d\gamma)^{16},(t^2+3)^{-66}),$$
$$((d\gamma)^{17},(t^2+3)^{-70}),((d\gamma)^{18},(t^2+3)^{-74}),((d\gamma)^{19},(t^2+3)^{-79}),((d\gamma)^{20},(t^2+3)^{-83}),$$
$$((d\gamma)^{21},(t^2+3)^{-87}),((d\gamma)^{22},(t^2+3)^{-91}),((d\gamma)^{23},(t^2+3)^{-95}),((d\gamma)^{24},(t^2+3)^{-99})\}$$

is a pseudo basis for a (t^2+3)*-maximal order since* $\mu_{(t^2+3)j} = \lceil -j(-21)/25\rceil, v_{(t^2+3)}(d) = 5$. *The discriminant of the* $(t+4)$*-maximal order described by the first pseudo basis above is* $(t+4)^{40}(t^2+3)^{600}$, *the discriminant of the* (t^2+3)*-maximal order described by the second pseudo basis above is divisible by* $(t+4)^{600}(t^2+3)^{128}$ *and the discriminant of the* $\{(t+4),(t^2+3)\}$*-maximal order generated by the concatenation of these pseudo bases, which is also the integral closure* $\mathbb{Z}_E^0$ *of* $k[t]$ *in* E, *is* $(t+4)^{40}(t^2+3)^{128}$.

Example 9. *Let* $F = \mathbb{F}_2(t), u = (t/(t^2+t+1),(t^6+t^4+t^3+1)/(t^6+t^5+t^3+t+1),1/t)$ *and* $S = \{(t),(t^2+t+1)\}$. *Then* $E = F(\wp^{-1}(u)) = F(\alpha) = F(\alpha_3)$. *The place* (t)

has ramification degree $p = 2$ and the place $(t^2 + t + 1)$ totally ramifies in E. We have $d_1 = t^2 + t + 1, d_2 = (t^2 + t + 1)^3, d = t(t^2 + t + 1)^6$ so $d_1\alpha_1, d_2\alpha_2$ and $d\alpha_3$ are all integral. The discriminant of $\mathbb{Z}_F[d\alpha_3]$ is divisible by $t^{64}(t^2 + t + 1)^{248}$.

We compute an Artin–Schreier–Witt quotient $\zeta = (t + 1, 0, 0)$ and Artin–Schreier quotient ρ by chinese remainder. Therefore

$$(\omega_{ij}, \mathfrak{a}_{ij}) = \{((d_1\alpha_1)^{i_1}(d_2\alpha_2)^{i_2}(d\alpha_3)^j, 1)\}_{0\le i_1,i_2<2,0\le j<2}$$

is a pseudo basis for a (t)-maximal order since $\mu_{(t)j} = \lceil -j(-1)/2 \rceil, v_{(t)}(d) = 1$ and

$$\begin{aligned}(\omega_{ij}, \mathfrak{a}_{ij}) = \{&(1, 1), (d(\alpha_3 - \rho), (t^2 + t + 1)^{-3}), ((d(\alpha_3 - \rho))^2, (t^2 + t + 1)^{-7}),\\ &((d(\alpha_3 - \rho))^3, (t^2 + t + 1)^{-11}), ((d(\alpha_3 - \rho))^4, (t^2 + t + 1)^{-15}),\\ &((d(\alpha_3 - \rho))^5, (t^2 + t + 1)^{-19}), ((d(\alpha_3 - \rho))^6, (t^2 + t + 1)^{-23}),\\ &((d(\alpha_3 - \rho))^7, (t^2 + t + 1)^{-27})\}\end{aligned}$$

is a pseudo basis for a $(t^2 + t + 1)$-maximal order since $\mu_{(t^2+t+1)j} = \lceil -j(-17)/8 \rceil$ and $v_{(t^2+t+1)}(d) = 6$. The discriminant of the (t)-maximal order described by the first pseudo basis above is $t^8(t^2 + t + 1)^{80}$, the discriminant of the $(t^2 + t + 1)$-maximal order described by the second pseudo basis above is divisible by $t^{64}(t^2 + t + 1)^{38}$ and the discriminant of the $\{(t), (t^2 + t + 1)\}$-maximal order described by the concatenation of these pseudo bases, which is the integral closure $\mathbb{Z}_E^0$ of $k[t]$ in E is $t^8(t^2 + t + 1)^{38}$.

Example 10. *Let $F = \mathbb{F}_3(t)[x]/\langle x^2 + t^3 + t + 1\rangle, u = ((t + 2)\lambda + 1/t^2, (t^3 + t^2)\lambda + 1/(t + 2), 1/t^2\lambda + t^6 + 2)$ where λ is a root of $x^2 + t^3 + t + 1$ and $S = \{(t), (t + 2, \lambda)\}$. Then $E = F(\wp^{-1}(u)) = F(\alpha) = F(\alpha_3)$ ([**Fra05**] Example 22). The place (t) totally ramifies in E and the place $(t + 2, \lambda)$ has ramification degree $p^2 = 9$. We have $d_1 = t^2, d_2 = t^6(t + 2)$ and $d = t^{18}(t + 2)^3$ so $t^2\alpha_1, t^6(t + 2)\alpha_2$ and $t^{18}(t + 2)^3\alpha_3$ are all integral. The discriminant of $\mathbb{Z}_F[d\alpha_3]$ is divisible by $t^{9540}(t + 2)^{3348}$.*

We compute an Artin–Schreier–Witt quotient $\zeta = (0,0,0)$ *and Artin–Schreier quotients* $\rho_{(t+2)} = 0, \rho_{(t)}$ *and* ρ *by chinese remainder. Therefore*

$$\begin{aligned}(\omega_{ij}, \mathfrak{a}_{ij}) = \{&((d_1\alpha_1)^i, 1), ((d_1\alpha_1)^i(d(\alpha_3-\rho)), (t+2,\lambda)^{-4}), ((d_1\alpha_1)^i(d(\alpha_3-\rho))^2, (t+2,\lambda)^{-8}),\\ &((d_1\alpha_1)^i(d(\alpha_3-\rho))^3, (t+2,\lambda)^{-13}), ((d_1\alpha_1)^i(d(\alpha_3-\rho))^4, (t+2,\lambda)^{-17}),\\ &((d_1\alpha_1)^i(d(\alpha_3-\rho))^5, (t+2,\lambda)^{-22}), ((d_1\alpha_1)^i(d(\alpha_3-\rho))^6, (t+2,\lambda)^{-26}),\\ &((d_1\alpha_1)^i(d(\alpha_3-\rho))^7, (t+2,\lambda)^{-31}), ((d_1\alpha_1)^i(d(\alpha_3-\rho))^8, (t+2,\lambda)^{-35})\}_{0\le i<3}\end{aligned}$$

is a pseudo basis for a $(t+2,\lambda)$*-maximal order since* $\mu_{(t+2,\lambda)j} = \lceil -j(-14)/9 \rceil, v_{(t+2),\lambda)}(d) = 6$ *and*

$$\begin{aligned}(\omega_{ij}, \mathfrak{a}_{ij}) = \{&(1,1), ((d(\alpha_3-\rho)), t^{-13}), ((d(\alpha_3-\rho))^2, t^{-26}), ((d(\alpha_3-\rho))^3, t^{-40}),\\ &((d(\alpha_3-\rho))^4, t^{-53}), ((d(\alpha_3-\rho))^5, t^{-67}), ((d(\alpha_3-\rho))^6, t^{-80}), ((d(\alpha_3-\rho))^7, t^{-94}),\\ &((d(\alpha_3-\rho))^8, t^{-107}), ((d(\alpha_3-\rho))^9, t^{-121}), ((d(\alpha_3-\rho))^{10}, t^{-134}), ((d(\alpha_3-\rho))^{11}, t^{-148}),\\ &((d(\alpha_3-\rho))^{12}, t^{-161}), ((d(\alpha_3-\rho))^{13}, t^{-175}), ((d(\alpha_3-\rho))^{14}, t^{-188}), ((d(\alpha_3-\rho))^{15}, t^{-202}),\\ &((d(\alpha_3-\rho))^{16}, t^{-215}), ((d(\alpha_3-\rho))^{17}, t^{-229}), ((d(\alpha_3-\rho))^{18}, t^{-242}), ((d(\alpha_3-\rho))^{19}, t^{-256}),\\ &((d(\alpha_3-\rho))^{20}, t^{-269}), ((d(\alpha_3-\rho))^{21}, t^{-283}), ((d(\alpha_3-\rho))^{22}, t^{-296}), ((d(\alpha_3-\rho))^{23}, t^{-310}),\\ &((d(\alpha_3-\rho))^{24}, t^{-323}), ((d(\alpha_3-\rho))^{25}, t^{-337}), ((d(\alpha_3-\rho))^{26}, t^{-350})\}\end{aligned}$$

is a pseudo basis for a (t)*-maximal order since* $\mu_{(t)j} = \lceil -j(-122)/27 \rceil, v_{(t)}(d) = 18$*. The discriminant of the* $(t+2,\lambda)$*-maximal order described by the first pseudo basis above is divisible by* $t^{3492}(t+2,\lambda)^{144}(t^2+1,\lambda+t)^{60}$*, the discriminant of the* (t)*-maximal order described by the second pseudo basis above is* $t^{390}(t+2,\lambda)^{1236}(t^2+1,\lambda+t)^{18}$ *and the discriminant of the* $\{(t+2,\lambda),(t)\}$*-maximal order generated by the concatenation of the two pseudo bases is divisible by* $t^{390}(t+2,\lambda)^{144}(t^2+1,\lambda+t)^{30}$*, the last prime being unramified with zero valuation in* u*.*

To compute the maximal order we take the unramified prime $(t^2+1,\lambda+t)$ *which occurs with exponent* 120 *in the discriminant of* $\mathbb{Z}_F[d\alpha_3]$ *and exponent* 30 *in the discriminant of the* $\{(t+2,\lambda),(t)\}$*-maximal order. The pseudo basis*

$$(\omega_{ij}, \mathfrak{a}_{ij}) = \{(\alpha_1^{i_1}\alpha_2^{i_2}\alpha_3^{i_3})_{0\le i_1,i_2,i_3<3}, (1)\}_{0\le i_1,i_2,i_3<3}$$

is a pseudo basis for an order which is maximal at any prime of F which does not ramify in E. The discriminant of this order is $t^{1404}(t+2,\lambda)^{432}$.

Adding these modules results in an order with discriminant $t^{390}(t+2,\lambda)^{144}$ which is the integral closure $\mathbb{Z}_E^0$ of $k[t]$ in E.

5.8. Timings

Due to the difficulty in testing whether a function field is an Artin–Schreier–Witt extension, the functionality available in Magma computes S-maximal orders and integral closures from a Witt vector or of an Artin–Schreier–Witt extension as a component of an abelian extension of a function field.

The timings we give below are for the computation of integral closures in Artin–Schreier–Witt extensions described by Witt vectors which includes the computation of an integral closure in the coefficient field E_{n-1}. We give timings for computing integral closures of $\mathbb{F}_p[t]$ in extensions of degree p^n of a rational function field in Tables 5.1 and 5.2 and for computing integral closures of $\mathbb{F}_p[t]$ in extensions of degree p^n of algebraic function fields ([**Fra05**] Examples 18-22, $F = \mathbb{F}_p(t)[x]/\langle x^2+t^3+t+1\rangle$ or when $p=2, F=\mathbb{F}_2(t)[x]/\langle x^3-x^2+2t-t^5\rangle$) in Table 5.3. The Witt vectors used for the timings in Table 5.1 are chosen so that there are 3 primes having the stated ramification degree and these appear with exponent 5 in the Witt vector when $p \leq 7$ and exponent 3 otherwise. When the ramification degree in these examples is p is the best case for Algorithm 9. The Witt vectors used for the timings in Table 5.2 are random and the extensions they define would most likely have a prime of each possible ramification degree. Such examples are not best case although they should avoid a discriminant calculation. The timings given in Table 5.2 are averages for the corresponding number of random examples stated in the "# examples" column.

The times in the "Algorithm 9" column are to be contrasted to the sum of the $\mathbb{Z}_{E_{n-1}}, \mathbb{Z}_{E_n}$ and "Transfer from $\mathbb{Z}_{E_n}$" columns, the sum of the "[**Fra05**]" and "Transfer from $\mathbb{Z}_{E_n}$" columns and the "Round 2" column.

Timings are given for an Intel(R) Core(TM) i7-3770 CPU 3.4GHz (32GB RAM) running Magma V2.20-8 under Linux.

Note that the computation of the discriminant for the $p=7, n=2, e=49$ example in Table 5.1 took 34.3hrs and that for the $p=3, n=3, e=27$ example took 2.5hrs.

p	n	$e(P'\|P)$, $P \in S$	$\mathbb{Z}_E$ by Algorithm 9	$\mathbb{Z}_{E_{n-1}}$	$\mathbb{Z}_{E_n}$	Transfer from $\mathbb{Z}_{E_n}$	Round 2
2	3	8	0.44s	0.01s	0.08s	0.01s	1.92s
2	3	4	0.16s	0.01s	0.06s	0.01s	0.88s
2	3	2	0.07s	0.0s	0.03s	0.0s	0.59s
2	4	16	61.96s	0.1s	16.09s	4.05s	405.88s
2	4	8	18.64s	0.06s	5.81s	1.43s	110.94s
2	4	4	4.32s	0.03s	0.91s	0.31s	38.58s
2	4	2	0.37s	0.0s	0.46s	0.12s	17.73s
2	5	8	1059s	0.94s	615.45s	138.7s	1.7hrs
2	5	2	28.05s	0.0s	13.25s	11.06s	989.61s
3	3	27	2.5hrs	0.01s	12.86s	264.66s	9.5hrs
3	3	9	68.07s	0.00s	0.91s	44.1s	2913.73s
3	3	3	3.55s	0.0s	0.21s	8.58s	604.24s
5	2	25	78.97s	0.0s	514.260s	54.76s	1.4hrs
5	2	5	2.97s	0.0s	0.05s	9.38s	366.99s
7	2	49	34.6hrs	0.0s	3.6s	1649.09s	138.9hrs
7	2	7	40.46s	0.0s	0.22s	186.62s	6.1hrs
11	2	11	2292.94s	0.0s	0.21s	5.1hrs	no attempt
13	2	13	3.8hrs	0.0s	0.5s	32.4hrs	no attempt

Table 5.1. Comparison of times for extensions of rational function fields

The degree 7^2 example in Table 5.3 using the Round 2 algorithm ran for more than 3 days. There are 72 primes it will compute a P-maximal order at and after 2 days it hadn't computed more than 2 such orders.

As can be seen in the examples involving taller towers of extensions corresponding to longer Witt vectors when the characteristic is small, Algorithm 9 does not compare favourably. Algorithm 9 is most efficient for larger characteristics and shorter towers of extensions (large p and small n) and also when the primes in the Witt vector are less ramified (ramification degree $\leq p$) avoiding a discriminant computation and maybe a strong approximation or chinese remainder in E_{n-1}. This advantage of avoiding the discriminant can be seen in Table 5.2 where it is likely that there is a prime of ramification degree p or 1 occurring in the random Witt vector. It can also be expensive to construct the order

p	n	# examples	$\mathbb{Z}_E$ by Algorithm 9	$\mathbb{Z}_{E_{n-1}}$	$\mathbb{Z}_{E_n}$	Transfer from $\mathbb{Z}_{E_n}$	Round 2
2	3	50	0.035s	0.001s	0.035s	0.004s	0.133s
2	4	50	1.948s	0.034s	2.059s	0.215s	9.502s
3	2	50	0.009s	0.0s	0.003s	0.004s	0.136s
3	3	50	8.636s	0.004s	0.695s	11.895s	301.701s
5	2	30	1.104s	0.000s	0.029s	2.548s	85.351s
7	2	30	31.129s	0.001s	0.208s	121.272s	5055.816s
11	2	5/5/5/5/1	65.9mins	0.006s	12.066s	7.5hrs	>1 day
13	2	4/2/2/1/0	6.3hrs	0.01s	64.44s	60.9hrs	no attempt

Table 5.2. Comparison of average times for random ASW extensions of rational function fields

p	n	$\mathbb{Z}_E$ by Algorithm 9	$\mathbb{Z}_{E_{n-1}}$	$\mathbb{Z}_{E_n}$	[**Fra05**]	Transfer from $\mathbb{Z}_{E_n}$	Round 2
3	2	0.09s	0.0s	0.11s	0.33s	0.07s	5.09s
5	2	3.77s	0.01s	1.4s	24.23s	28.47s	789.39s
7	2	109.7s	0.01s	32.7s	34.3hrs	1862.25s	>3 days
2	3	1.71s	0.04s	18.44s	4.48s	0.47s	113.05s
3	3	140.75s	0.12s	94.37s	804.66s	226.24s	2157.62s

Table 5.3. Comparison of times for examples from [**Fra05**]

from the basis even when the basis is in normal form. Computing an integral basis can be done sometimes much faster than computing the integral closure itself.

We have also compared timings for some examples with a prototype of [**Bau14**] which is not restricted to any particular type of extension. For a number of examples our implementation of Algorithm 9 is faster than his integral closure implementation. In particular our implementation was much faster than his when the ramification of the primes was small and in some cases of small ramification our implementation was able to compute integral closures in less than 1.5hrs when his did not in 2 days ($p = 13, n = 2$).

Chapter 6

Applications to Coding Theory

In this chapter we give an example and some timings for computations of integral closures in Abelian extensions and examples of how the more efficient integral closure computations described in this thesis improve the construction of Algebraic–Geometric codes from cyclic extensions.

Timings are given for an Intel(R) Core(TM)2 i7-3770 CPU 3.4GHz (32GB RAM) machine running Magma V2.20-9 under Linux.

6.1. Abelian Extensions

We give an example of an Abelian extension which has components which are Kummer, Artin–Schreier and Artin–Schreier–Witt extensions.

Example 11. *Let $F = \mathbb{F}_3(t), D = 4P_{(t+1)}$, R the ray class group of D and U the subgroup of the ray class group of D generated by the generator of R of order 3 plus 4 times the free generator of R. We compute an abelian extension $A = F[x_1, x_2, x_3]/\langle f_1, f_2, f_3\rangle$ where $f_1 = x_1^2 + 2t(t+1), f_2 = x_2^9 + 2t^3x_2^6 + 2t^5x_2^4 + (2t^6 + 2t^5)x_2^3 + 2t^7x_2^2 + t^7x_2 + t^9 + 2t^7 + 2t^6$ and $f_3 = x_3^3 + 2x_3 + 2t/(t+1)$. Let α_i be a root of f_i. The discriminant of the finite equation order $\mathbb{F}_3[t][\alpha_1, \alpha_2, (t+1)\alpha_3]$ is $t^{459}(t+1)^{135}$. A pseudo basis for the finite maximal order of the Kummer extension of degree 2 in A is*

$$B_1 = \{(1,1), (\alpha_1, 1)\}$$

since $\mu_{P,j} = 0$ for $P = t, t+1$. A pseudo basis for the finite maximal order of the Artin–Schreier extension of degree 3 in A is

$$B_3 = \{(1,1), ((t+1)\alpha_3, 1), (((t+1)\alpha_3)^2, (t+1)^{-1})$$

since $\mu_{(t+1),j} - jv_{t+1}(d) = \lceil -j(-1)/3 \rceil - j$. A pseudo basis for the finite maximal order of the Artin–Schreier–Witt extension of degree 3^2 is

$$B_2 = \{(1,1), (t\alpha_2, 1), ((t\alpha_2)^2, t^{-1}), (\gamma, 1), (t\alpha_2\gamma, 1), ((t\alpha_2)^2\gamma, t^{-1}), (\gamma^2, 1), (t\alpha_2\gamma^2, 1), ((t\alpha_2)^2\gamma^2, t^{-1})\}$$

since $\mu_{t,j} - jv_t(d) = \lceil -j(-1)/3 \rceil - j$. *We take the product* $\{B_{1,j}B_{2,l}B_{3,m}\}_{\{0\le j<2, 0\le l<9, 0\le m<3\}}$ *of these bases and compute the order of* A *with this basis which has discriminant* $t^{99}(t+1)^{99}$. *The discriminant of the maximal order of the abelian extension is known to be* $t^{81}(t+1)^{81}$. *We complete the computation by doing Round 2 steps on the almost maximal order given by the product basis.*

6.2. Coding Theory

How Geometric Goppa codes or Algebraic–Geometric codes can be constructed from divisors of a function field is explained in Chapter 2 of [**Sti93**]. A simple example of the construction of an Algebraic–Geometric code from an abelian extension of a function field and one of its divisors is given in Section 4.3 of [**Fie06**]. By computing the maximal orders of the abelian extension directly and avoiding the computation of the maximal orders of the function field of the abelian extension using the Round 2 algorithm we show that the use of our algorithms improves the efficiency of constructing such codes. The Magma code from [**Fie06**] can be accessed at http://magma.maths.usyd.edu.au/magma/dmwm/. When a function field is constructed from an abelian extension we essentially replace

```
K := FunctionField(AbelianExtension(D_opt, U_opt));
```

in that code with

```
A := AbelianExtension(D_opt, U_opt);
K := FunctionField(A);
time MaximalOrderFinite(A);
time MaximalOrderInfinite(A);
```

to use Algorithm 2 instead of Round 2 on the equation orders of K for the maximal order computations. Since we are computing codes from cyclic extensions below this replacement may be unnecessary.

A table of genera and number of rational points on curves over a range of constant field sizes can be found at www.manypoints.org. We notice that the number of rational points compared to the genus increases with size of constant field hence we use some larger constant fields in our examples. The data given at this website is the best known. The codes we have constructed do not attempt to match this best known ratio between the genus and the number of rational points rather we choose examples with a good ratio where the function fields are cyclic extensions which shows the improvement which is available in the code construction when using the integral closure algorithms described in Chapters 2, 3 and 5.

We give some information and timings in Tables 6.1 to 6.9 for constructing codes in $\mathbb{F}_q^m$, where m is the number of rational points, using both Algorithm 2 and Round 2 for the computation of the integral closures. We report

- the number m of rational points of the function field,
- the genus g of the function field,
- the time taken to compute each of the integral closures using both algorithms.

To construct the codes below from a function field we add together all the rational places and construct a divisor G coprime to the rational places. From [**Sti93**] Corollary II.2.3 we have that the sum of the dimension of the code and the minimum distance of the code is bounded below by $m+1-g$. This is why we would like to have small genus compared to the number of rational points. But this sum is bounded above by $m+1$ ([**Sti93**] Proposition II.1.7 (Singleton Bound)) so there is an inverse relationship between the dimension and minimum distance. For given number of rational points and genus a larger dimension code will have a smaller minimal distance and vice versa. For each code we report

- the dimension of the code,
- the designed distance $m - \deg(G)$ of the code which is a lower bound for the minimum distance,
- the time to compute the rational places,
- the time to compute the Riemann–Roch space of G and
- the time to evaluate the basis of this Riemann–Roch space at the m rational places.

The code constructed is the set of vectors $\{(x(P_1), \ldots, x(P_m)) \mid x \in \mathcal{L}(G)\} \subset \mathbb{F}_q^m$ where $\mathcal{L}(G)$ is the Riemann–Roch space of G and $P_1, \ldots, P_m$ are the rational places.

$F = \mathbb{F}_{11^2}(t)[x]/\langle x^{11} + 10x + (w^{30}t^6 + w^{14}t^5 + w^{30}t^4 + w^{37}t^3 + t^2 + w^{16}t)/ (t^6 + t^5 + w^{37}t^4 + w^{16}t^3 + w^{118}t^2 + w^{26}t + w^{46})\rangle, \mathbb{F}_{11^2} = \mathbb{F}_{11}\langle w\rangle$					
$G = \sum_{5 \text{ places } P'\mid P} P' + P'_{t^3+w^{41}t^2+w^{53}t+w^7}, P = P_{t^3+t^2+w^{114}t+w^{56}}$					
m	g	Finite		Infinite	
		Algo. 2	Round 2	Algo. 2	Round 2
242	35	0.01s	0.12s	0.0s	0.0s
	Dimension	Designed Distance	Rational Places	Riemann–Roch space	Evaluation
	65	143	0.13s	0.01s	0.35s

Table 6.1. Constructing a code contained in $\mathbb{F}_{11^2}^{242}$

$F = \mathbb{F}_{37}(t)[x]/\langle x^{37} + 36x + (t^2 + 16t + 1)(t)(t^2 + 13t + 14)^{-2}(36)\rangle$					
$G = (t^2 + 18t + 30)$					
m	g	Finite		Infinite	
		Algo. 2	Round 2	Algo. 2	Round 2
148	72	0.07s	21.27s	0.01s	0.01s
	Dimension	Designed Distance	Rational Places	Riemann–Roch space	Evaluation
	21	74	0.8s	0.0s	1.35s

Table 6.2. Constructing a code contained in $\mathbb{F}_{37}^{148}$

$F = \mathbb{F}_{71}(t)[x]/\langle x^{71} + 70x + (40t^2 + 14t + 1)(t)(t^2 + 38t + 7)^{-2}(70)\rangle$					
$G = (t^2 + 5t + 40)$					
m	g	Finite		Infinite	
		Algo. 2	Round 2	Algo. 2	Round 2
284	140	0.53s	836.26s	0.07s	0.07s
	Dimension	Designed Distance	Rational Places	Riemann–Roch space	Evaluation
	38	142	11.48s	0.02s	13.8s

Table 6.3. Constructing a code contained in $\mathbb{F}_{71}^{284}$

$F = \mathbb{F}_{83}(t)[x]/\langle x^{83} + 82x + (71t^2 + 65t + 1)(t)(t^2 + 32t + 11)^{-2}(82)\rangle$					
$G = (t^2 + 60t + 71)$					
m	g	Finite		Infinite	
		Algo. 2	Round 2	Algo. 2	Round 2
332	164	0.89s	2462.98s	0.1s	0.1s
	Dimension	Designed Distance	Rational Places	Riemann–Roch space	Evaluation
	44	166	34.79s	0.01s	24.49s

Table 6.4. Constructing a code contained in $\mathbb{F}_{83}^{332}$

As can be seen from these timings by using our efficient algorithms we have removed a substantial contribution to the time taken to construct some codes from cyclic extensions.

$F = \mathbb{F}_{97}(t)[x]/\langle x^{97} + 96x + (25t^2 + 30t + 1)(t)(t^2 + 33 * t + 9)^{-2}(96)\rangle$					
$G = (t^2 + 90t + 46)$					
m	g	Finite		Infinite	
		Algo. 2	Round 2	Algo. 2	Round 2
388	192	1.49s	2.1 hrs	0.14s	0.15s
	Dimension	Designed Distance	Rational Places	Riemann–Roch space	Evaluation
	51	194	84.82s	0.03s	44.11s

Table 6.5. Constructing a code contained in $\mathbb{F}_{97}^{388}$

$F = \mathbb{F}_{5^5}(t)[x]/\langle x^{71} + (t^2 + w^{328}t + w^{931})^{67}(t^2 + w^{1393}t + w^{2617})^4(w)(4)\rangle$, $\mathbb{F}_{5^5} = \mathbb{F}_5\langle w\rangle$					
$G = (t^2 + w^{1747}t + w^{1422}) + (t^2 + w^{631}t + w^{1850}) + (t^2 + w^{2792}t + w^{1023})$					
m	g	Finite		Infinite	
		Algo. 2	Round 2	Algo. 2	Round 2
3266	70	0.37s	2501.55s	0.07s	0.06s
	Dimension	Designed Distance	Rational Places	Riemann–Roch space	Evaluation
	357	2840	552.2s	0.95s	93.91s

Table 6.6. Constructing a code contained in $\mathbb{F}_{5^5}^{3266}$

It is possible to gain an isomorphic field by swapping x and t in the construction of these extensions. This may produce a smaller degree extension in which case this may lead to a more efficient way of constructing the code. We note that this is not the case in Table 6.9 as the field is degree 121 in its current representation and degree 242 if defined over $\mathbb{F}_{3^5}(x)$.

$F = \mathbb{F}_{2^9}(t)[x]/\langle x^{73} + (t^2 + w^{419}t + w^{367})^{72}(t)^{40}(t^2 + w^{333}t + w^{173})\rangle$, $\mathbb{F}_{2^9} = \mathbb{F}_2\langle w\rangle$					
$G = (t^2 + w^{259}t + w^{361}) + (t^2 + w^{325}t + w^6) + (t^2 + w^{491}t + w^{333})$					
m	g	Finite		Infinite	
		Algo. 2	Round 2	Algo. 2	Round 2
730	72	0.09s	1558.21s	0.07s	637.63s
	Dimension	Designed Distance	Rational Places	Riemann–Roch space	Evaluation
	367	292	23.27s	0.57s	20.73s

Table 6.7. Constructing a code contained in $\mathbb{F}_{2^9}^{730}$

$F = \mathbb{F}_{2^{11}}(t)[x]/\langle x^{89} + (t^2 + w^{931}t + w^{1391})^{78}(t^2 + w^{746}t + w^{1844})^{11}(w)\rangle$, $\mathbb{F}_{2_{11}} = \mathbb{F}_2\langle w\rangle$					
$G = (t^2 + w^{374}t + w^{823}) + (t^2 + w^{188}t + w^{198}) + (t^2 + w^{1941}t + w^{113})$					
m	g	Finite		Infinite	
		Algo. 2	Round 2	Algo. 2	Round 2
1780	88	0.42s	3 hrs	0.1s	0.12s
	Dimension	Designed Distance	Rational Places	Riemann–Roch space	Evaluation
	447	1246	182.47s	1.02s	82.04s

Table 6.8. Constructing a code contained in $\mathbb{F}_{2^{11}}^{1780}$

$F = \mathbb{F}_{3^5}(t)[x]/\langle x^{121} + u\rangle, \mathbb{F}_{3^5} = \mathbb{F}_3\langle w\rangle$					
$G = (t^2 + w^{179}t + w^{137})$					
m	g	Finite		Infinite	
		Algo. 2	Round 2	Algo. 2	Round 2
484	120	0.55s	6.4 hrs	0.24s	0.25s
	Dimension	Designed Distance	Rational Places	Riemann–Roch space	Evaluation
	123	242	184.54s	0.47s	47.49s

Table 6.9. Constructing a code contained in $\mathbb{F}_{3^5}^{484}$

6.2.1. Data. Here we provide the information which did not fit into the tables above. The fields and divisors used in these examples were chosen from randomly generated fields and divisors for their good code generating properties, not for the ability to fit their data into a table.

From Table 6.1, let α be a root of the defining polynomial of F, then the divisor G was $(t^3 + t^2 + w^{114}t + w^{56}, (t^3 + 6t^2 + w^{51}t + w^{83})\alpha + w^{95}t^2 + w^{44}t + w^{53}) + (t^3 + t^2 + w^{114}t + w^{56}, (t^3 + 6t^2 + w^{51}t + w^{83})\alpha + w^{25}t^2 + w^{88}t + w^{28}) + (t^3 + t^2 + w^{114}t + w^{56}, (t^3 + 6t^2 + w^{51}t + w^{83})\alpha + w^{89}t^2 + w^{82}t + w^{31}) + (t^3 + t^2 + w^{114}t + w^{56}, (t^3 + 6t^2 + w^{51}t + w^{83})\alpha + w^{2}t^2 + w^{83}t + w^{71}) + (t^3 + t^2 + w^{114}t + w^{56}, (t^3 + 6t^2 + w^{51}t + w^{83})\alpha + w^{21}t^2 + w^{115}t + w^{73}) + (t^3 + t^2 + w^{114}t + w^{56}, (t^3 + 6t^2 + w^{51}t + w^{83})\alpha + w^{4}t^2 + w^{75}t + w^{90}) + (t^3 + t^2 + w^{114}t + w^{56}, (t^3 + 6t^2 + w^{51}t + w^{83})\alpha + w^{90}t^2 + w^{117}t + 1) + (t^3 + t^2 + w^{114}t + w^{56}, (t^3 + 6t^2 + w^{51}t + w^{83})\alpha + w^{104}t^2 + w^{14}t + w^{44}) + (t^3 + t^2 + w^{114}t + w^{56}, (t^3 + 6t^2 + w^{51}t + w^{83})\alpha + w^{82}t^2 + 9t + w^{38}) + (t^3 + t^2 + w^{114}t + w^{56}, (t^3 + 6t^2 + w^{51}t + w^{83})\alpha + w^{51}t^2 + w^{97}t + w^{39}) + (t^3 + t^2 + w^{114}t + w^{56}, (t^3 + 6t^2 + w^{51}t + w^{83})\alpha + w^{79}t^2 + w^{18}t + w^{94}) + (t^3 + w^{41}t^2 + w^{53}t + w^{7}) + (t^3 + w^{50}t^2 + w^{63}t + w^{116})$.

From Table 6.9, the field F has defining polynomial $x^{121} + u$ where $u = w^{122}t^{242} + w^{21}t^{241} + w^{194}t^{240} + w^{101}t^{239} + t^{238} + w^{173}t^{237} + w^{72}t^{236} + w^{213}t^{235} + w^{144}t^{234} + w^{59}t^{233} + w^{200}t^{232} + w^{131}t^{231} + w^{38}t^{230} + w^{179}t^{229} + w^{110}t^{228} + w^{9}t^{227} + w^{150}t^{226} + w^{81}t^{225} + w^{214}t^{224} + w^{113}t^{223} + w^{44}t^{222} + w^{193}t^{221} + w^{92}t^{220} + w^{23}t^{219} + w^{164}t^{218} + w^{63}t^{217} + w^{236}t^{216} + w^{175}t^{215} + w^{74}t^{214} + w^{5}t^{213} + w^{154}t^{212} + w^{53}t^{211} + w^{226}t^{210} + w^{125}t^{209} + w^{24}t^{208} + w^{197}t^{207} + w^{112}t^{206} + w^{11}t^{205} + w^{184}t^{204} + w^{91}t^{203} + w^{232}t^{202} + w^{163}t^{201} + w^{62}t^{200} + w^{203}t^{199} + w^{134}t^{198} + w^{25}t^{197} + w^{166}t^{196} + w^{97}t^{195} + w^{4}t^{194} + w^{145}t^{193} + w^{76}t^{192} + w^{217}t^{191} + w^{116}t^{190} + w^{47}t^{189} + w^{156}t^{188} + w^{55}t^{187} + w^{228}t^{186} + w^{135}t^{185} + w^{34}t^{184} + w^{207}t^{183} + w^{106}t^{182} + w^{5}t^{181} + w^{178}t^{180} + w^{93}t^{179} + w^{234}t^{178} + w^{165}t^{177} + w^{72}t^{176} + w^{213}t^{175} + w^{144}t^{174} + w^{43}t^{173} + w^{184}t^{172} + w^{115}t^{171} + w^{6}t^{170} + w^{147}t^{169} + w^{78}t^{168} + w^{227}t^{167} + w^{126}t^{166} + w^{57}t^{165} + w^{198}t^{164} + w^{97}t^{163} + w^{28}t^{162} + w^{39}t^{161} + w^{180}t^{160} + w^{111}t^{159} + w^{18}t^{158} + w^{159}t^{157} + w^{90}t^{156} + w^{231}t^{155} + w^{130}t^{154} + w^{61}t^{153} + w^{218}t^{152} + w^{117}t^{151} + w^{48}t^{150} + w^{197}t^{149} + w^{96}t^{148} + w^{27}t^{147} + w^{168}t^{146} + w^{67}t^{145} + w^{240}t^{144} + w^{131}t^{143} + w^{30}t^{142} + w^{203}t^{141} + w^{110}t^{140} + w^{9}t^{139} + w^{182}t^{138} + w^{81}t^{137} + w^{222}t^{136} + w^{153}t^{135} + w^{92}t^{134} + w^{233}t^{133} + w^{164}t^{132} + w^{71}t^{131} + w^{212}t^{130} + w^{143}t^{129} + w^{42}t^{128} + w^{183}t^{127} + w^{114}t^{126} + w^{29}t^{125} + w^{170}t^{124} + w^{101}t^{123} + w^{8}t^{122} + w^{149}t^{121} + w^{80}t^{120} + w^{221}t^{119} + w^{120}t^{118} + w^{51}t^{117} + w^{184}t^{116} + w^{83}t^{115} + w^{14}t^{114} + w^{163}t^{113} + w^{62}t^{112} + w^{235}t^{111} + w^{134}t^{110} + w^{33}t^{109} + w^{206}t^{108} + w^{73}t^{107} + w^{214}t^{106} + w^{145}t^{105} + w^{52}t^{104} + w^{193}t^{103} + w^{124}t^{102} + w^{23}t^{101} + w^{164}t^{100} + w^{95}t^{99} + w^{10}t^{98} + w^{151}t^{97} + w^{82}t^{96} + w^{231}t^{95} + w^{130}t^{94} + w^{61}t^{93} + w^{202}t^{92} + w^{101}t^{91} + w^{32}t^{90} + w^{165}t^{89} + w^{64}t^{88} + w^{237}t^{87} + w^{144}t^{86} + w^{43}t^{85} + w^{216}t^{84} + w^{115}t^{83} + w^{14}t^{82} + w^{187}t^{81} + w^{224}t^{80} + w^{123}t^{79} + w^{54}t^{78} + w^{203}t^{77} + w^{102}t^{76} + w^{33}t^{75} + w^{174}t^{74} + w^{73}t^{73} + w^{4}t^{72} + w^{161}t^{71} + w^{60}t^{70} + w^{233}t^{69} + w^{140}t^{68} + w^{39}t^{67} + w^{212}t^{66} + w^{111}t^{65} + w^{10}t^{64} + w^{183}t^{63} +$

$$w^{74}t^{62}+w^{215}t^{61}+w^{146}t^{60}+w^{53}t^{59}+w^{194}t^{58}+w^{125}t^{57}+w^{24}t^{56}+w^{165}t^{55}+w^{96}t^{54}+w^{35}t^{53}+$$
$$w^{176}t^{52}+w^{107}t^{51}+w^{14}t^{50}+w^{155}t^{49}+w^{86}t^{48}+w^{227}t^{47}+w^{126}t^{46}+w^{57}t^{45}+w^{214}t^{44}+w^{113}t^{43}+$$
$$w^{44}t^{42}+w^{193}t^{41}+w^{92}t^{40}+w^{23}t^{39}+w^{164}t^{38}+w^{63}t^{37}+w^{236}t^{36}+w^{127}t^{35}+w^{26}t^{34}+w^{199}t^{33}+$$
$$w^{106}t^{32}+w^{5}t^{31}+w^{178}t^{30}+w^{77}t^{29}+w^{218}t^{28}+w^{149}t^{27}+w^{16}t^{26}+w^{157}t^{25}+w^{88}t^{24}+w^{237}t^{23}+$$
$$w^{136}t^{22}+w^{67}t^{21}+w^{208}t^{20}+w^{107}t^{19}+w^{38}t^{18}+w^{195}t^{17}+w^{94}t^{16}+w^{25}t^{15}+w^{174}t^{14}+w^{73}t^{13}+w^{4}t^{12}+$$
$$w^{145}t^{11}+w^{44}t^{10}+w^{217}t^{9}+w^{108}t^{8}+w^{7}t^{7}+w^{180}t^{6}+w^{87}t^{5}+w^{228}t^{4}+w^{159}t^{3}+w^{58}t^{2}+w^{199}t+w^{130}.$$

Part 2

Galois Groups of Polynomials over Global Function Fields

Chapter 7

Algorithms for Computing Galois Groups

In this chapter we describe a general algorithm for computing Galois groups of irreducible polynomials over global fields, (Algorithm 11). This algorithm is a generalization of the algorithm of Fieker and Klüners [**FK14**] which was originally developed to compute Galois groups of polynomials over $\mathbb{Q}$. Our purpose is to compute Galois groups of polynomials over global function fields and in Chapter 8 we expand on our description of Algorithm 11 for this case. A particular difficulty in generalizing [**FK14**] is that for some groups G and H the invariants provided are S_n-invariant when the characteristic is 2 and so are never G-relative H-invariants (Definition 7.2). For such groups G and H we state in this thesis (Section 8.5) some new polynomials which are G-relative H-invariant when the characteristic is 2. These invariants are a key contribution to this part of the thesis.

Geißler [**Gei03**] provides an algorithm for Galois groups of polynomials of degree at most 23 over $\mathbb{Q}$ and $k(t)$. This was the most recent work on algorithms for Galois groups when Fieker and Klüners [**FK14**] developed their algorithm for Galois groups of polynomials over $\mathbb{Q}$. Unlike most previous algorithms the algorithm of [**FK14**] is not degree restricted, it can compute the Galois group of any polynomial over any algebraic number field or algebraic function field (including of course $\mathbb{Q}$ and $k(t)$ for $k = \mathbb{F}_q, \mathbb{Q}$). Hulpke [**Hul99**] is not degree restricted either, however, it usually cannot determine the Galois group uniquely. The algorithm of [**FK14**] has been implemented in Magma [**CBFS10**] V2.13 for polynomials over $\mathbb{Q}$ and in V2.14 for polynomials over number fields and $\mathbb{Q}(t)$.

We describe in this chapter the algorithm of [**FK14**]. We have implemented this algorithm in Magma [**CBFS10**] for polynomials over $\mathbb{F}_q(t)$ (V2.16) and global algebraic function fields (simple extensions of $\mathbb{F}_q(t)$) (V2.17). This is the first implementation, of which we know, of an algorithm for computing Galois groups over global function fields which is not restricted by the degree of the polynomial. It is also the first algorithm (that we know of) which uses the computation of subfields (and in particular the generating subfields as introduced by Klüners, van Hoeij and Novocin [**vHKN11**]) of global function fields in calculating the Galois group. This algorithm is based on [**Sta73**].

The results in this part of this thesis also appear in [**Sut15**].

We begin with some definitions.

Definition 7.1. *The* Galois group, $\mathrm{Gal}(f)$, *of a polynomial f over a field F is the automorphism group of S_f/F where S_f is the splitting field of f over F.*

When f is irreducible over F and of degree n we compute Galois groups as transitive subgroups of S_n, the *symmetric group* of degree n containing all permutations of n objects. Such a group will permute the n roots of f. A group G of permutations of the n elements of the set Ω, is *transitive* if for all elements $x, y \in \Omega$ there is a $g \in G$ such that $gx = y$.

A right *coset* of a subgroup H of G is $Hx = \{hx : h \in H\}$ for $x \in G$. A *permutation representation* of G which acts on a set of cardinality l is a homomorphism from G into S_l. A *wreath product* $J \wr H$ of the group J by the group H with respect to the action of H on the set Ω containing n elements is the semi-direct product $\{(j, h) | j \in J^n, h \in H\}$ with $(j_1, h_1)(j_2, h_2) = (j_1 j_2^{h_1^{-1}}, h_1 h_2)$, where $j_2^{h_1^{-1}}$ is the action of the permutation inverse to h_1 on the n elements of J in j_2.

Invariants and resolvents are an important part of our algorithm. We define invariants and resolvents here and discuss the uses of the different types later. Let R be a commutative unitary domain and $I(x_1, \ldots x_n) \in R[x_1, \ldots x_n]$. A permutation $\tau \in S_n$ acts on I by permuting $x_1 \ldots, x_n$ and we write I^τ for this action.

Definition 7.2. *A polynomial $I(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ such that $I^\tau = I$ for all $\tau \in H$ for some group $H \subseteq S_n$ is said to be* H-invariant.

A H-invariant polynomial $I(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ is a G-relative H-invariant *polynomial if $I^\tau \neq I$ for all $\tau \in G \setminus H, H \subset G \subseteq S_n$, that is, for the stabiliser in G we have* $\mathrm{Stab}_G I = H$.

For a G-relative H-invariant polynomial I we can compute a G-relative H-invariant resolvent polynomial

$$Q_{(G,H)}(y) = \prod_{\tau \in G//H} (y - I^\tau(x_1, \ldots, x_n)),$$

where $G//H$ denotes a right transversal*, a system of representatives for the right cosets $H\tau$, of G/H. If $G = S_n$ then we call Q an* absolute resolvent*, otherwise we call Q a* relative resolvent.

An S_n-relative H-invariant is a G-relative H-invariant and a G-relative H-invariant is a H-invariant but the converse is not always true.

We recall the definition of a block system as it is crucial to the definition of a number of our special invariants, (we use Geißler and Klüners ([**GK00**] Definition 2.14)).

Definition 7.3. *Let G be a transitive permutation group acting on a finite set Ω. A subset $\emptyset \neq \Delta \subset \Omega$ is called a* block *if $\Delta \cap \Delta^\sigma \in \{\emptyset, \Delta\}$ for all $\sigma \in G$. The orbit of a block Δ under G is called a* block system.

A group G is called primitive *if it has only trivial blocks, $\{1\}, \ldots, \{n\}$ and $\{1, \ldots, n\}$, otherwise it is called* imprimitive.

The blocks we use will be subsets of $\Omega = \{\text{roots of } f\}$. A block system of a group G is a block system for the transitive subgroups of G but the converse does not always hold. The action of a group G which permutes the blocks of G gives a transitive permutation representation. Let $\bar{G}$ denote the image of this representation which, when used for this purpose, essentially maps from S_n into some $S_l, l \mid n$.

7.1. Previous Work

Our algorithm is similar to that of Geißler and Klüners [**GK00**] and Geißler [**Gei03**]. They use many of the same techniques that we do. Their algorithm is also based on Stauduhar [**Sta73**] and uses relative resolvents. They use subfields, short cosets and p-adic methods in their algorithm also. However, their algorithm can only be applied to polynomials of degree less than 15 [**GK00**] and degree less than 23 [**Gei03**].

The method of Stauduhar [**Sta73**] is also used by Eichenlaub and Olivier [**Eic96**] who implemented their algorithm in Pari for polynomials of degree up to 11.

Another method is that of the absolute resolvent. Such resolvents can be computed from coefficients of polynomials and a factorization may give enough information about the Galois group to identify it. However, for degrees larger than say 11, these factorizations can be rather expensive. For algorithms using this method see [**Soi81, SM85, MM97, CM94**].

The absolute resolvent method can be combined with the method of Stauduhar as a verification step. This is described in [**GK00, Gei03**]. It is used when the index of the maximal subgroup H in G, a group which we know contains the Galois group, is large and we choose to use a smaller precision for the approximations of the roots of the polynomial than required for a proven descent to shorten the running time of the algorithm and leave the proof of the descent step from G to H till later (if indeed we decided that the Galois group may be contained in H), see Section 8.8.

The use of p-adic approximations in the method of Stauduhar was first suggested by Yokoyama [**Yok97**]. Such approximations were also used by Darmon and Ford [**DF89**] independently of Stauduhar's method. Previous to this complex approximations to roots

of rational polynomials were used which required higher precisions to obtain proven results. We have extended the idea of p-adic splitting fields in our choice of splitting fields for polynomials over rational function fields.

7.2. A Recent Algorithm for Computing Galois Groups

We describe here the algorithm used by Fieker and Klüners [**FK14**] with no degree restrictions. A similar algorithm was used by [**Gei03**] and [**GK00**].

Let f be a separable polynomial of degree n over a field F with splitting field S_f over F. An F-automorphism of S_f will permute the roots of f and this permutation will determine the automorphism completely, therefore we represent Galois groups as groups of permutations acting on the roots of f in some fixed ordering. When f is irreducible we know that the Galois group of f will be a transitive subgroup of S_n (because each root can be mapped to any of the others by an automorphism) [**DS00**], the task is to discover which one.

The algorithm of Stauduhar [**Sta73**] traverses maximal subgroups until it finds one the Galois group is contained in or finds that the Galois group is contained in no maximal subgroup so must be the group we know it is contained in. Maximal subgroups are computed in Magma [**CBFS10**] using an algorithm by Cannon and Holt [**CH04**].

Theorem 7.4 (Stauduhar [**Sta73**])**.** *Let $f(x)$ be a separable polynomial of degree n over a field F. Let $\alpha_1, \ldots, \alpha_n$ be a fixed ordering of the roots of $f(x)$ in S_f. Suppose that with respect to the given ordering of the roots, the Galois group $\mathrm{Gal}(f)$ of $f(x)$ is a subgroup of a group G. Let H be a subgroup of G and $I(x_1, \ldots, x_n) \in R[x_1, \ldots, x_n]$ be a G-relative H-invariant polynomial. Let $\tau_1, \ldots, \tau_l$ be representatives for the right cosets of H in G. For all $i, I^{\tau_i}(\alpha_1, \ldots, \alpha_n)$ is a root of the resolvent polynomial*

$$Q_{(G,H)}(y) = \prod_{i=1}^{l} (y - I^{\tau_i}(\alpha_1, \ldots, \alpha_n)) \in F[y].$$

Assume $I^{\tau_i}(\alpha_1, \ldots, \alpha_n)$ is not a repeated root of $Q_{(G,H)}(y)$. Then $\mathrm{Gal}(f) \subseteq \tau_i H \tau_i^{-1}$ iff $I^{\tau_i}(\alpha_1, \ldots, \alpha_n) \in F$.

For polynomials $f \in \mathbb{F}_q(t)[x]$ this means that $I^{\tau_i}(\alpha_1, \ldots, \alpha_n)$ is a rational function instead of an algebraic function. The above theorem is a generalization of Theorem 5 of [**Sta73**] which is stated for irreducible polynomials, transitive groups and $F = \mathbb{Q}$.

Stauduhar considers roots of f in the complex field, however it is more efficient to compute roots of f in the splitting field of f over the completion of F at some finite place

P which is what the algorithms of [**GK00**], [**Gei03**] and [**FK14**] do following [**Yok97**]. This approach also generalizes more easily between number fields and function fields.

For more detail about the steps in Algorithm 11 see Chapter 8.

Algorithm 11 (Compute the Galois Group of an irreducible polynomial)**.**
Input:

- *An irreducible separable polynomial f of degree n over an algebraic number field or algebraic function field F (including $\mathbb{Q}, \mathbb{F}_q(t)$ or $\mathbb{Q}(t)$).*

Output:

- *The Galois group of f.*

Steps:

1. *Choose a finite place P of F such that the image of f is squarefree over the residue field at P.*
2. *Find a scaling factor s such that $s\alpha_i$ is integral ($s\alpha_i \in \mathbb{Z}, \mathbb{F}_q[t], \mathbb{Q}[t]$ or a finite extension thereof) for all roots α_i of f. Each $s\alpha_i$ will be a root of $f_s = s^{n-1}f(x/s)$.*
3. *Compute the splitting field $S_{f,P}$ for f over the completion of F at the prime P.*
4. *Compute the roots of f in $S_{f,P}$ to low precision to fix an ordering.*
5. *Find a group G which the Galois group of f is contained in (S_n will always do here, although we can sometimes do better) :*
   (a) *Compute the generating subfields* [**vHKN11**] *of the field extension $F[x]/f$ and the Galois groups of the normal closures of these subfields.*
   (b) *Compute the intersection of the wreath products corresponding to the block system in* [**GK00**] *Theorem 3.1, of $S_{n/l}$ with the Galois groups of the normal closures of subfields of degree l for all subfields of $F[x]/f$.*
6. *While G has maximal subgroups which could contain* $\mathrm{Gal}(f)$
   (a) *For each conjugacy class of maximal subgroups of G, compute a G-relative H-invariant polynomial for a representative maximal subgroup H of the conjugacy class.*
   (b) *Compute a cost for deciding whether* $\mathrm{Gal}(f)$ *is contained in the groups in each conjugacy class. For a representative subgroup H, let the cost c_H be the product of the number of cosets of G/H, the number of multiplications in the G-relative H-invariant chosen and a bound on the evaluation of the invariant at the roots $s\alpha_i$ of f_s (Section 8.8).*

(c) *Apply Theorem 7.4 : For the conjugacy class of maximal subgroups of G with smallest cost c_H not yet decided on do*
  (i) *Let H be a representative maximal subgroup from the conjugacy class.*
  (ii) *Retrieve the G-relative H-invariant polynomial $I \in R[x_1, \ldots x_n]$ computed in Step (6a) and any Tschirnhaus transformation T selected in a previous iteration (Step 6(c)vB).*
  (iii) *Compute the precision m needed in the roots of f for transformation by T then evaluation in I.*
  (iv) *Compute the roots of f to precision m in the splitting field $S_{f,P}$.*
  (v) *for the representatives $\tau \in G//H$ of the right cosets of H in G*
    (A) *Evaluate I at the transformed roots $T(s\alpha_i)$ of f_s permuted by τ where α_i has been computed in Step 6(c)iv.*
    (B) *Decide whether this evaluation is the image of an element of F. If so then the resolvent has a root in F and if it is a single root $\mathrm{Gal}(f) \subseteq \tau H \tau^{-1}$ so set $G = \tau H \tau^{-1}$ and restart the loop (6) with the new G. If the resolvent has a root in F but it is not a single root then a descent into this conjugacy class may be re-attempted after applying another Tschirnhausen transformation. Choose a transformation randomly and update the cost c_H for this transformation.*

7. *Return G.*

An improvement to the algorithm above is to use the short cosets $G/_\sigma H = \{H\tau : \sigma \in H\tau\}$ of H in G which contain the subgroup corresponding to the Frobenius automorphism σ instead of the whole transversal $G//H$ in Step 6(c)v, ([**GK00**] Section 4 and [**Els14a**]). However, if we use this approach to tackle the problems posed by maximal subgroups of large index we cannot determine whether the resolvent has a single root in F. If we find a double root of the resolvent using only the short cosets then we can try the descent again with another Tschirnhausen transformation. If we find no roots using the short cosets then we need no longer consider this conjugacy class of subgroups. Otherwise it is possible but not proven that the Galois group of f is contained in $\tau H \tau^{-1}$. This can be proven later. In an attempt to get more accurate results we ensure that there is a minimum number of cosets (say 20) used for this shortcut.

In the next chapter we give details about which places will lead to the most efficient computation (Step 1, Section 8.1), the splitting field that will be used for the computation of the roots of the polynomial and the mapping into that splitting field (Step 3, Section 8.2),

a group to start the computations with (Step 5, Section 8.3), the invariants we can use (dependent on characteristic) (Step 6(c)ii, Section 8.4), Tschirnhausen transformations (Step 6(c)ii and 6(c)vB, Section 8.7), the computation of a bound and a precision necessary to use that bound to determine whether the evaluation of an invariant at the roots of f to the precision calculated is in F (Step 6b, 6(c)iii and 6(c)vB, Section 8.8).

Let $\mathbb{Z}_F^0$ be the integral closure of R in F, where $R \subset F$ is one of $\mathbb{Z}, \mathbb{F}_q[t]$ or $\mathbb{Q}[t]$. The scaled polynomial f_s is monic and integral, that is $f_s \in \mathbb{Z}_F^0[x]$, and the relationships between its roots are the same as between the roots of f. The roots of a monic, integral polynomial will be integral and so have finite expansions in the splitting field over a completion.

Chapter 8

Galois Groups of Irreducible Polynomials

Here we describe the steps of Algorithm 11 considering especially its use for polynomials over a function field with characteristic p. Let f be a polynomial of degree n with coefficients in F. We give greater detail for $F = \mathbb{F}_q(t)$ or $F = \mathbb{F}_q(t)(\alpha)$ where $q = p^e$ for some e and α is algebraic over $\mathbb{F}_q(t)$. (Any function field $\mathbb{F}_q(t)(\alpha)(\beta)$ is isomorphic to a function field of the form $\mathbb{F}_q(t)(\gamma)$ for some γ). We will attempt to keep our description as general as possible and will note when the details we give are specific to F being a global function field and if these details are specific to F being a rational or algebraic function field.

8.1. Choosing a Good Place (Algorithm 11, Step 1)

The place $P \subset F$ which we use to compute a completion which we extend to a splitting field will affect the performance of our algorithm. In fact, by trying out several places we can frequently collect enough cycle lengths to determine the Galois group itself, if the Galois group is A_n or S_n, which it often is [**DS00**].

We require that P is finite, unramified in $F[x]/f$ and does not divide the leading coefficient or denominators of f. We compute the residue field K of P ($= \mathbb{F}_{q^r}$ for some r when F is a global function field) and factor $\bar{f}$, the image of f over K, over K. We check $\bar{f}$ is squarefree over K to ensure P is unramified and we can Hensel lift distinct roots. Such a place will exist because these conditions are equivalent to the discriminant of f having valuation zero at P and the discriminant will have non-zero valuation at only finitely many places.

To choose P, we loop through a limited number of places, at most $10n$ when F is a global function field. We collect the degrees of the factors of $\bar{f}$ over K and the LCMs (d_P) of these degrees multiplied by the degree r_P of P. The degrees are cycle lengths of elements in the Galois group ([**GK00**], Remark 2.4). If there is a cycle of some prime length $n/2 < l < n-2$ then the Galois group is S_n or A_n ([**Ser03**], Corollary 10.2.2). If a group does not contain elements with these cycle lengths then it is not the Galois group of f. We can use this test to eliminate groups cheaply from our list of possibilities.

To obtain a ring over the completion $K[[\rho]]$ of $\mathbb{Z}_F^0$ at P which contains all roots of f over $K[[\rho]]$ when F is a global function field we first compute the splitting field $E = \mathbb{F}_{(q^{r_P})^{d_P}}$ for $\bar{f}$ over K. We would like arithmetic in $E[[\rho]]$ to be not too expensive as we find roots in $E[[\rho]]$ and evaluate invariants at roots in $E[[\rho]]$. The precision necessary for the roots of f is inversely related to the degree r_P of the place P. So a larger r_P will allow us to work with roots with less precision but this may make E itself large and expensive to work in. We attempt to take a middle ground to balance these factors.

We make use of the Frobenius automorphism σ of $E/\mathbb{F}_q$ so we attempt to compute E large enough so that σ is non trivial. To do this we consider the number of cycles, that is, the number of factors, $l_{f,P}$, of f over the residue class field at P. Given a group G which we know contains the Galois group and a maximal subgroup H we would usually need to test $[G : H]$ many evaluations $I^\tau(\alpha_1, \ldots, \alpha_n)$ for some invariant I. Knowledge of a non trivial σ allows us to reduce this number to the number of $\tau \in G//_\sigma H = \{\tau : \sigma \in H^\tau\}$. This is the use of short coset systems as described in [**GK00**] Section 4 and [**Els14a**].

Therefore, when F is a global function field we choose a place P with the smallest $r_P d_P l_{f,P}^{1.5} > n/4$, if such occurs as a place we have considered, otherwise a place we have considered with largest $r_P d_P l_{f,P}^{1.5} \leq n/4$.

8.2. Computing Roots (Algorithm 11, Step 3 and 6(c)iv)

Let F be a global function field. We construct $E = \mathbb{F}_{(q^{r_P})^{d_P}} = \mathbb{F}_{q^{r_P d_P}}$ where $\bar{f}$ splits into linear factors. Let ρ be the image of P in $E[[\rho]]$. We use the map $h : F \to E[[\rho]]$ given by the completion mapping at P into $K[[\rho]]$ followed by the inclusion into $E[[\rho]]$. We can find the roots $\bar{\alpha}_i$ of f in $E[[\rho]]$ using Puiseux expansions as in [**Duv89**] which is implemented in Magma [**CBFS10**] or by computing the roots of $\bar{f}$ in the finite field E and using any root lifting technique. This shows that f splits in $E[[\rho]]$.

8.2.1. Mapping back to the Function Field (Algorithm 11 Step 6(c)vB). In Section 8.8, we use the map $h_m^r : K[[\rho]]/\rho^m \to F/(P^m)$, given by the inverse of the completion mapping followed by rational reconstruction (or reduction when F is a rational function field) modulo P^m. The map h_m^r is applied to the evaluation of invariants at roots of f_s in $E[[\rho]]$. If the result of an evaluation of an invariant at the roots of f lies in $E[[\rho]] \setminus K[[\rho]]$ then the evaluation does not map back to F.

8.3. A Starting Group (Algorithm 11, Step 5)

If the discriminant of f is a square in F (and the characteristic $p \neq 2$) then the Galois group is contained in A_n otherwise it is not ([**Sta73**], [**vdW66**] p. 155 Exercise 4). This is equivalent to the use of the SqrtDisc invariant (Theorem 8.4) but cheaper.

We looked at the SqrtDisc invariant (Theorem 8.1) in a similar way for the characteristic 2 case. The discriminant of a polynomial contains information about the roots of the polynomial but can be computed from the coefficients. In the characteristic 2 case we could not compute an element of F related to the SqrtDisc invariant without computing the roots of the polynomial which is too expensive in general for a check which is supposed to be a shortcut.

However, it is possible that the computation of the subfields and the wreath products of their Galois groups with $S_{n/l}$ for a degree l subfield may give us a starting group contained in A_n if the Galois group is contained in A_n. So if $F[x]/f$ has subfields then the discriminant check may not provide any unique information. If the characteristic is 2 and $F[x]/f$ has no subfields then we do not currently have an easier way to determine whether we can descend from S_n to A_n than Algorithm 11 Step 6c.

Note that it is also possible to use the factorization of the 2-set or 2-sum resolvent of f, the monic polynomial whose roots are the products or sums of pairs of roots of f, to compute a smaller starting group [**CM94**] but we do not have nor have we implemented algorithms to do this in characteristic p.

8.3.1. Subfields (Algorithm 11, Step 5a, 5b). Knowing the subfields of the extension $F[x]/f$ can speed our computation of the Galois group of f. In some cases knowing the subfields enables the Galois group to be computed in reasonable time where this would not be possible otherwise. It can avoid the need to check some expensive descents by reducing the starting group to a subgroup of large enough index in S_n.

For a subfield L of degree l of $F' = F[x]/f$ we have that $\mathrm{Gal}(f) \subseteq \mathrm{Gal}(g') \wr \mathrm{Gal}(g) \subseteq S_{n/l} \wr S_l$ where g is the polynomial defining the subfield L/F and g' is a defining polynomial for F'/L. We have $|A \wr B| = |A|^l|B|$ when $B \subseteq S_l$ but computing $\mathrm{Gal}(g)$ is easier than computing $\mathrm{Gal}(g')$. We use the approximation for the second factor to gain a smaller starting group, that is, $\mathrm{Gal}(f) \subseteq S_{n/l} \wr \mathrm{Gal}(g)$, (this is the largest group having the block system of the subfield which specifies which roots of f combine to give roots of g) and since this holds for all subfields L of F' we have that $\mathrm{Gal}(f) \subseteq \cap_L S_{n/l_L} \wr \mathrm{Gal}(g_L)$ where l_L is the

degree of the subfield L and g_L is a defining polynomial for L. This is explained at length in [**GK00**], Section 3.

A general subfields algorithm which also applies to global function fields has recently been developed by Klüners, van Hoeij and Novocin [**vHKN11**]. This algorithm can also compute subfields of algebraic function fields represented as an extension of another algebraic function field. This occurs here when F is an algebraic function field. So we are now able to compute and use subfields to improve the efficiency of computing Galois groups over global function fields.

In [**vHKN11**] subfields are computed by taking intersections of some *generating subfields*, subfields which cannot be obtained by intersecting larger subfields. They explain how to find a set of subfields such that all subfields of a function field $F' = F[x]/f$ can be computed as the intersection of these generating subfields. For our purposes we can use just the generating subfields in the Galois group computation, any other subfields will be subfields of (at least) two of the generating subfields so may be computed in any recursion. By factoring the polynomial f over $F[x]/f$ we compute *principal subfields* of $F[x]/f$. Some of these subfields will be generating subfields but there will be no more of them than there are factors of f over $F[x]/f$.

8.4. Invariants (Algorithm 11, Step 6(c)ii)

Let $\mathrm{Gal}(f) \subseteq G \subseteq S_n$. For each maximal subgroup H of G we choose a G-relative H-invariant. There are a number of different types of invariants which have been used and which we continue to use. They fall into 3 categories : special, generic and combinations. Generic invariants will work for all groups G and their maximal subgroups H. Special invariants can only be used when the groups G and H satisfy certain properties, however, they are the cheaper invariants and we should use them when we can. Combination invariants combine invariants for 2 other subgroups to obtain an invariant for a third, they are cheaper than generic invariants and some special invariants. In contrast to some previous algorithms we compute our invariants as we require them rather than looking them up in a table. This is what makes the algorithm of [**FK14**] degree independent.

We are guaranteed to be able to find an invariant. We know from [**GK00**] that

$$I(\underline{X}) = \sum_{\tau \in H} (\prod_{i=1}^{n-1} X_i^i)^\tau$$

is always a G-relative H-invariant (it is a generic invariant). It is not an efficient one although sometimes it is the best we can do. [**GK00**] also states that using an invariant

of smallest total degree has major effects on the efficiency of the algorithm, that multiplications are expensive and the number of them should be minimized and that we can gain during the lifting procedure by using an invariant whose resolvent has smaller absolute value roots. [**FK14**] and [**Els12**] look for invariants which also have a small number of terms or operations. The larger the degree of the invariant the larger will be the bound in Step 6b and the larger will be the precision we then need to work with. So it is important that we choose our G-relative H-invariants carefully.

Now that we are working with polynomials in characteristic p the invariants are in $\mathbb{F}_q[t][X_1, \ldots, X_n]$ and because of this some polynomials which are relative invariants in characteristic 0 are no longer relative invariants in some positive characteristics. Fortunately we have found this to be the case only in characteristic 2, as we prove in the theorems in Section 8.6, and in some cases we have found formulas for polynomials with similar invariant properties which we can use instead (Section 8.5).

Below we give formulas for polynomials which are special G-relative H-invariants for certain pairs of groups G and H. Most of these can be found in [**Gei03**], [**GK00**] or [**FK14**]. However we will first look at formulas for polynomials which are G-relative H-invariants for some $H < G$ only in characteristic 2, (Theorems 8.1 and 8.2). Each of these will be analogous to a formula for a polynomial which is G-relative H-invariant for some $H < G$ in all other characteristics, (Theorems 8.4 and 8.5). Theorem 8.3 contains formulas for invariants which are G-relative in all characteristics. We will also show that the more expensive but guaranteed to exist generic invariants remain G-relative in characteristic 2 (Theorem 8.6).

8.5. Invariants in Characteristic 2

In this section we state polynomials and prove that they are relative invariants when the characteristic of F is 2. These polynomials are derived from or inspired by similar polynomials which are known to be relative invariants when the characteristic of F is 0 but are invariant for a larger group than required when the characteristic of F is 2.

Theorem 8.1. *Let H be a maximal subgroup of $G \subseteq S_n$. Then, when the characteristic of F is 2, the following gives polynomials $I(\underline{X}) = I(X_1, \ldots, X_n)$ which are G-relative H-invariant polynomials when G and H satisfy the conditions given.*

SqrtDisc: *When $H < A_n, G \not< A_n$*

$$I(\underline{X}) = \prod_{1 \le j < j' \le n} (X_j + \bar{u} X_{j'}) = I_1 + \bar{u} I_2 \text{ [Els13a]}$$

where I_1 and I_2 are also G-relative H-invariant and $\bar{u}$ is the image of u in $\mathbb{F}_2[u]/\langle u^2-1\rangle$ and

$$I(\underline{X}) = \sum_{1\le j<j'\le n} X_j \frac{\prod_{1\le r<s\le n}(X_r+X_s)}{X_j+X_{j'}}$$

although the former is the most efficient.

D: *When H has the same block systems as G, G is a subgroup of $S_{n/l} \wr_\Gamma S_l$ for some $l|n$ H is a subgroup of $S_{n/l} \wr_\Gamma A_l$, $\Gamma = \{1,\dots,l\}$,*

$$I(\underline{X}) = E(\underline{y}),$$

where E is either I, I_1 or I_2 from the [**Els13a**] *SqrtDisc invariant above and*

$$I(\underline{X}) = \sum_{1\le j<j'\le \#B} y_j \frac{\prod_{1\le r<s\le \#B}(y_r+y_s)}{y_j+y_{j'}},$$

where $B = \{b_j\}_{1\le j\le l}$ is a block system of both G and H, $\#b_j = n/l$, $y_j = \sum_{i\in b_j} X_i$ and $\underline{y} = (y_1,\dots,y_l)$.

$\mathbf{s_1} \equiv \mathbf{s_m}$: *When G is a subgroup of $S_{n/l} \wr_\Gamma S_l$ for some $l|n$, $\Gamma = \{1,\dots,l\}$ there is a subgroup H with the same block systems as G such that*

$$(s_m) \qquad I(\underline{X}) = \prod_{b\in B} E(\{X_j : j\in b\})$$

is a G-relative H-invariant polynomial where E is the SqrtDisc ([**Els13a**]*) invariant I (not I_1 or I_2) and*

$$(s_1) \qquad I(\underline{X}) = \sum_{b\in B}\Big(\sum_{j,j'\in b, j<j'} \frac{X_j}{X_j+X_{j'}}\Big)$$

is a G-relative H-invariant function where $B = \{b_i\}_{1\le i\le l}$ is a block system of both G and H, $\#b_i = n/l$.

Note that in parallel with [**FK14**] Theorem 5.7 the inner function of the $s_1 \equiv s_m$ invariant (the SqrtDisc function) could be replaced by any U-relative N-invariant polynomial E satisfying $E^\sigma = \bar{u}E$ (s_m) or $E^\sigma = E+1$ (s_1) for all $\sigma \in U \setminus N$ where $G = U \wr V$ and $N < U$ is normal of index 2, (the I_1 and I_2 invariants of the [**Els13a**] SqrtDisc invariant and the SqrtDisc invariant do not satisfy these properties). While (s_1) is the s_1 polynomial summing over blocks in a system, in characteristic 2 it acts the same way as the s_m polynomial does in other characteristics (which multiplies over blocks in a system). However such polynomials E over $\mathbb{F}_q[t]$ have not been found and so this invariant is not used in the Magma [**CBFS10**] implementation. The situation of (s_m) is covered by the

implementation of Factor Delta invariants by [**Els14b**]. Using Theorem 8.2 we can then get an invariant similar to $\mathrm{D\,s_m}$ in Theorem 8.4.

Proof. **SqrtDisc** [**Els13a**]**:** Any permutation is a product of transpositions so we look here at the action of a single transposition. Let $\tau = (r, s) \in S_n$ be a transposition,

$$I^\tau(\underline{X}) = \prod_{1\le j<j'\le n, j, j' \notin \{r,s\}} (X_j + \bar{u}X_{j'}) \prod_{1\le j<j'\le n, j \text{ or } j' \in \{r,s\}} (X_{j^\tau} + \bar{u}X_{j'^\tau}).$$

The first product is invariant under τ so we look at the second. Let $r < s$, then this second product is

$$\begin{aligned}
&(X_{r^\tau} + \bar{u}X_{s^\tau}) \prod_{r<j\le n, j\ne s} (X_{r^\tau} + \bar{u}X_{j^\tau}) \prod_{1\le j'<s, j'\ne r} (X_{j'^\tau} + \bar{u}X_{s^\tau}) \\
&= (X_s + \bar{u}X_r) \prod_{r<j\le n, j\ne s} (X_s + \bar{u}X_j) \prod_{1\le j'<s, j'\ne r} (X_{j'} + \bar{u}X_r) \\
&= \bar{u}(X_r + \bar{u}X_s) \prod_{r<j<s} (X_s + \bar{u}X_j) \prod_{s<j\le n} (X_s + \bar{u}X_j) \prod_{1\le j'<r} (X_{j'} + \bar{u}X_r) \prod_{r<j'<s} (X_{j'} + \bar{u}X_r) \\
&= \bar{u}(X_r + \bar{u}X_s) \prod_{r<j<s} \bar{u}(X_j + \bar{u}X_s) \prod_{s<j\le n} (X_s + \bar{u}X_j) \prod_{1\le j'<r} (X_{j'} + \bar{u}X_r) \prod_{r<j'<s} \bar{u}(X_r + \bar{u}X_{j'})
\end{aligned}$$

The middle 2 products appear in $I(\underline{X})$, but not in the first product in I^τ above. The first and last products have the same number of factors (which all appear in I and not in the first product of I^τ above) so the $\bar{u}$ here will cancel out, which means we are left with the one $\bar{u}$ out the front. So we have $I^\tau = \bar{u}I$. Therefore I is not τ-invariant. However, if a second transposition σ was applied to I we would have $I^{\tau\sigma} = \bar{u}I^\sigma = \bar{u}\bar{u}I = I$, therefore I is H-invariant for any $H < A_n$ and G-relative for $G \not< A_n$.

To see that I_1 and I_2 are also G-relative H-invariant we start with $I^\tau = \bar{u}I$. Then

$$\begin{aligned}
(I_1 + \bar{u}I_2)^\tau &= \bar{u}(I_1 + \bar{u}I_2) \\
I_1^\tau + \bar{u}I_2^\tau &= \bar{u}I_1 + \bar{u}^2 I_2
\end{aligned}$$

Equating coefficients of $\bar{u}$ gives $I_1^\tau = I_2$ and $I_2^\tau = I_1$. Note that $I_1 \ne I_2$ otherwise I is invariant under τ which we have proved above is not the case. Therefore neither I_1 nor I_2 are τ invariant but $I_1^{\tau\sigma} = I_2^\sigma = I_1$ therefore I_1 and similarly I_2 are A_n invariant.

SqrtDisc : For the second SqrtDisc invariant we proceed in a similar fashion. We split the invariant into 2 parts, we write

$$I(\underline{X}) = (\sum_{1\le j<j'\le n} \frac{X_j}{X_j + X_{j'}}) \prod_{1\le r<s\le n} (X_r + X_s)$$

and note that the second factor is S_n-invariant. Let I_1 be the first factor and let $\tau = (r, s)$ be a transposition,

$$\begin{aligned} I_1^\tau(\underline{X}) &= \sum_{1\le j<j'\le n} \frac{X_{j^\tau}}{X_{j^\tau} + X_{j'^\tau}} \\ &= \sum_{1\le j<j'\le n, j, j'\notin\{r,s\}} \frac{X_{j^\tau}}{X_{j^\tau} + X_{j'^\tau}} + \sum_{1\le j<j'\le n, j \text{ or } j'\in\{r,s\}} \frac{X_{j^\tau}}{X_{j^\tau} + X_{j'^\tau}} \end{aligned}$$

and we note that the first sum is invariant under τ. We continue with the second assuming $r < s$,

$$\begin{aligned} &\sum_{1\le j<j'\le n, j \text{ or } j'\in\{r,s\}} \frac{X_{j^\tau}}{X_{j^\tau} + X_{j'^\tau}} \\ &= \sum_{r<j\le n, j\ne s} \frac{X_{r^\tau}}{X_{r^\tau} + X_{j^\tau}} + \sum_{1\le j'<s, j'\ne r} \frac{X_{j'^\tau}}{X_{j'^\tau} + X_{s^\tau}} + \frac{X_s}{X_s + X_r} \\ &= \sum_{r<j\le n, j\ne s} \frac{X_s}{X_s + X_j} + \sum_{1\le j'<s, j'\ne r} \frac{X_{j'}}{X_{j'} + X_r} + \frac{X_s}{X_s + X_r} \\ &= \sum_{r<j<s} \frac{X_s}{X_s + X_j} + \sum_{s<j\le n} \frac{X_s}{X_s + X_j} + \sum_{1\le j'<r} \frac{X_{j'}}{X_{j'} + X_r} + \sum_{r<j'<s} \frac{X_{j'}}{X_{j'} + X_r} + \frac{X_s}{X_s + X_r} \end{aligned}$$

The 2nd and 3rd sums appear in $I_1(\underline{X})$ but not in the first sum of I_1^τ above, the first and fourth sums have the same number of terms but none of their addends appear in I_1. However,

$$\frac{X_j}{X_{j'} + X_j} = \frac{X_{j'}}{X_{j'} + X_j} + 1$$

so the first sum becomes

$$\sum_{r<j<s} (\frac{X_j}{X_s + X_j} + 1)$$

and similarly for the fourth sum. Because they have the same number of terms adding the first and the fourth sum now gives

$$\sum_{r<j<s} \frac{X_j}{X_j + X_s} + \sum_{r<j'<s} \frac{X_r}{X_{j'} + X_r}$$

where the $+1$ cancel since there are an even number of them and the terms in this sum all appear in $I_1(\underline{X})$ and not in any part of $I^\tau(\underline{X})$ which we have already considered. This leaves us with the last term

$$\frac{X_s}{X_s + X_r} = \frac{X_r}{X_s + X_r} + 1$$

so that $I_1^\tau = I_1 + 1$ and hence I_1 is not invariant under τ and so not S_n-invariant. But $I_1^{\tau\sigma} = (I_1 + 1)^\sigma = I_1 + 2 = I_1$ so I_1 and also I are H-invariant for $H < A_n$ and G-relative for any $G \not< A_n$.

D: We follow the hint in [**FK14**] following Theorem 5.7. We can use [**FK14**] Lemma 5.4, the E invariant, where E is the polynomial of the SqrtDisc invariant for S_m and A_m since the transitive permutation representations which permute the blocks are subgroups of S_m and A_m.

$\mathbf{s_1}$: Since this invariant acts in the same way as the s_m invariant in other characteristics we will refer to the proof of Theorem 5.7 of [**FK14**]. Replacing $-d_i$ by $d_i + 1$, $\pm F$ by F or $F + 1$ and $F^{u_1} = -F$ by $F^{u_1} = F + 1$ in that proof we have that $I(\underline{X})$ is a G-relative H-invariant.

$\mathbf{s_m}$: Replacing $-d_i$ by $\bar{u}d_i$, $\pm F$ by F or $\bar{u}F$ and F^{u_1} by $\bar{u}F$ in the proof of Theorem 5.7 of [**FK14**] we have that $I(\underline{X})$ is a G-relative H-invariant.

□

The SqrtDisc invariant is important when $\mathrm{Gal}(f)$ is primitive. This corresponds to the stem field $F[x]/f$ having no subfields (such as when the degree of f is prime) which means that Algorithm 11 Step 5 cannot gain a smaller starting group. It also means there are no non-trivial block systems of any $G \supseteq \mathrm{Gal}(f)$ so none of the other special invariants can be used as they all use block systems. In characteristic 2 we cannot use whether the discriminant is a square to determine whether or not the Galois group of f is a subgroup of A_n which would mean that in characteristic 2 if there are no subfields and no non trivial block systems then without a SqrtDisc invariant we could only use the more expensive generic invariants to attempt to descend all the way from S_n.

Theorem 8.2 ([**Fie09**])**.** *Let $H_1, H_2 \subset G \subseteq S_n$ be two distinct subgroups of index 2 in G with G-relative H_i-invariants I_i, $G//H_i = \{\mathrm{Id}, \tau_i\}$. Then, when the characteristic of F is 2,*

$$I(\underline{X}) = \begin{cases} I_1 + I_2, & \text{if } I_i^{\tau_i} = I_i + 1 \\ I_1 I_2^{\tau_2} + I_2 I_1^{\tau_1} & \text{otherwise} \end{cases}$$

is a G-relative H-invariant where $H = \langle H_1 \cap H_2, \tau_1\tau_2 \rangle$.

Proof. ([**Fie09**]) The first formula follows easily from substitution into the second, however the proof for the second follows from a substitution into the first which is simpler to prove so we will prove only the first and note the necessary substitution.

Assume $I_i^{\tau_i} = I_i + 1$, then we have resolvent polynomials $R_i = x^2 + (I_i^{\tau_i} + I_i)x + I_i^{\tau_i} I_i = x^2 + x + I_i^2 + I_i$. These resolvent polynomials define quadratic Artin–Schreier extensions of the invariant ring $\mathbb{F}_q[t](\underline{X})^G$ ([**FK14**] Remark 2.1). Since there are 2 such extensions there must be a third and by Artin–Schreier theory $x^2 + x + I_1^2 + I_1 + I_2^2 + I_2$ is a generating polynomial for the third quadratic subfield of the degree 4 extension generated by R_i with Galois group $V_4 \cong C_2 \times C_2$. Its roots will be primitive elements in the extension and as such will be invariants. Therefore $I_1 + I_2$ (and $I_1 + I_2 + 1$) are G-relative H-invariants for some index 2 subgroup H. It can easily be seen that $I(\underline{X})$ is both $H_1 \cap H_2$-invariant and invariant under $\tau_1\tau_2$ so $H \supset \langle H_1 \cap H_2, \tau_1\tau_2 \rangle$. Since $\langle H_1 \cap H_2, \tau_1\tau_2 \rangle$ has index 2 in G we must have that $H = \langle H_1 \cap H_2, \tau_1\tau_2 \rangle$.

To prove the second formula repeat the above argument with $\tilde{I}_i = I_i/(I_i + I_i^{\tau_i})$, since $\tilde{I}_i^{\tau_i} = \tilde{I}_i + 1$. Then we have that

$$x^2 + x + \frac{I_1 I_1^{\tau_1}}{(I_1 + I_1^{\tau_1})^2} + \frac{I_2 I_2^{\tau_2}}{(I_2 + I_2^{\tau_2})}$$

is a generating polynomial for the third quadratic subfield of the degree 4 extension generated by the R_i with Galois group V_4 and using the transformation $x \mapsto x/(I_1 + I_1^{\tau_1})(I_2 + I_2^{\tau_2})$ and clearing denominators we have that $x^2 + (I_1 + I_1^{\tau_1})(I_2 + I_2^{\tau_2})x + I_1 I_1^{\tau_1}(I_1 + I_1^{\tau_1})^2 + I_2 I_2^{\tau_2}(I_2 + I_2^{\tau_2})^2$ is also a generating polynomial for that subfield and it can be seen that $I_1 I_2^{\tau_2} + I_2 I_1^{\tau_1}$ and $I_1 I_2^{\tau_2} + I_2 I_1^{\tau_1} + 1$ are roots of that polynomial and hence are G-relative H-invariants. □

8.6. Invariants in Characteristic other than 2

In this section we state polynomials and prove that they are relative invariants either when the characteristic of F is $p > 0$ or $p > 2$. These polynomials are known to be relative invariants when the characteristic of F is 0.

Theorem 8.3. *Let H be a maximal subgroup of $G \subseteq S_n$. Then for all characteristics of F, the following gives polynomials $I(\underline{X}) = I(X_1, \ldots, X_n)$ which are G-relative H-invariant polynomials when G and H satisfy the conditions given.*

Intransitive, [FK14] Lemma 5.1: *When H is an intransitive group and there is an orbit $\mathcal{O}$ of H which is not invariant under G,*

$$I(\underline{X}) = \sum_{i \in \mathcal{O}} X_i.$$

ProdSum, [Gei03] Algorithm 6.24 Step 3.1, [FK14] Lemma 5.3, [Els14b]: *When there exists a block system B of H which is not a block system of G,*

$$I(\underline{X}) = \prod_{b \in B} (\sum_{i \in b} X_i) \text{ and } I(\underline{X}) = \sum_{b \in B} (\sum_{i \in b} X_i)^e$$

where $e = 2$ unless $p = 2$ then $e = 3$.

E, [Gei03] Satz 6.14, Algorithm 6.24 Step 4.1.2: *When H has the same block systems as G, $\overline{H} < \overline{G}$ are transitive permutation representations on l points which permute the blocks in a block system,*

$$I(\underline{X}) = E(y_1, \ldots, y_l)$$

where $y_j = \sum_{i \in B_j} X_i$, $B = \{B_1, \ldots, B_l\}$ is a block system for G and H and E is a $\overline{G}$-relative $\overline{H}$-invariant.

F, [Gei03] Satz 6.16, Algorithm 6.24 Step 4.1.4: *When H has the same block systems as G, $\overline{H} = \overline{G}$, $\mathrm{Stab}_H(B_i)|_{B_i} < \mathrm{Stab}_G(B_i)|_{B_i}$ for $B_i = \{b_{i1}, \ldots, b_{il}\}$ a block in the block system $B = \{B_1, \ldots, B_r\}$ of G and H,*

$$I(\underline{X}) = \sum_{\tau_j \in \tau} \tilde{F}^{\tau_j}(X_{b_{i1}}, \ldots, X_{b_{il}})$$

where $\tilde{F}$ is a $\mathrm{Stab}_G(B_i)|_{B_i}$-relative $\mathrm{Stab}_H(B_i)|_{B_i}$-invariant and τ is a system of representatives of left cosets of $\mathrm{Stab}_H(B_i)$.

BlockQuotient, [Gei03] Algorithm 6.24, Step 6, [FK14] Lemma 5.6:
When H has the same block systems as G, $\overline{H} = \overline{G}$, $\mathrm{Stab}_H(B_i)|_{B_i} = \mathrm{Stab}_G(B_i)|_{B_i}$ for all blocks B_i in the block system B of G and H,

$$I(\underline{X}) = f(\underline{Y}) \text{ where } \underline{Y} = \mathrm{Orb}_G(Y)$$

where f is a $G|_{\underline{Y}}$-relative $H|_{\underline{Y}}$-invariant and Y is a K_2-relative K_1-invariant polynomial for some groups $K_1 < K_2 < \mathrm{Stab}_G(B_i)|_{B_i}$ and $H|_{\underline{Y}} < G|_{\underline{Y}}$.

Proof. We mostly refer to existing proofs but note dependence on the characteristic.

Intransitive: Let $h \in H$, $I^h(\underline{X}) = \sum_{i \in \mathrm{Orb}_H(1)} X_{i^h} = I(\underline{X})$ since $i^h \in \mathrm{Orb}_H(1)$ as the orbit is invariant under H. Let $g \in G \setminus H$, $I^g(\underline{X}) = \sum_{i \in \mathrm{Orb}_H(1)} X_{i^g}$. Since the orbit is not invariant under G, there exists i such that $i^g \notin \mathrm{Orb}_H(1)$ therefore $I^g \neq I$. Therefore I is a G-relative H-invariant polynomial independent of the characteristic.

ProdSum: The first formula is proved to be a G-relative H-invariant independent of characteristic in [**FK14**] Lemma 5.3, so we will give a similar proof for the second formula which contains less multiplications and is characteristic dependent. Let $h \in H$, $I^h(\underline{X}) = \sum_{b \in B} (\sum_{i \in b} X_{i^h})^e$. Since B is a block system $h \in H$ will only reorder either the outer sum or all of the inner sums which leaves I invariant under H. However $g \in G \setminus H$ will map X_i and X_j with i, j in different blocks to the same block so that I^g contains a monomial $X_{i^g} X_{j^g}$ which is not present in I. Note that if in characteristic 2 we used $e = 2$ such monomials (with coefficient $e = 2$) would not be present for any i, j and the invariant would be only a sum of squares which would also be G-invariant and so not G-relative.

E: A proof that this $I(\underline{X})$ is a G-relative H-invariant is given in both [**Gei03**] Satz 6.14 and [**FK14**] Lemma 5.4. Note that addition of indeterminates is independent of characteristic and that E is an invariant chosen dependent on the characteristic of F.

F: A proof that this $I(\underline{X})$ is a G-relative H-invariant is given in both [**Gei03**] Satz 6.16 and [**FK14**] Lemma 5.5. Note that addition of indeterminates is independent of characteristic and that $\tilde{F}$ is an invariant chosen dependent on the characteristic of F.

BlockQuotient: This invariant $I(\underline{X})$ is discussed in [**Gei03**] Bemerkung 6.19 and in [**FK14**] Lemma 5.6. Note that f and Y will be chosen dependent on the characteristic and that evaluation is independent of characteristic.

□

Theorem 8.4. *When the characteristic of F is not 2, the following gives polynomials $I(\underline{X}) = I(X_1, \ldots, X_n)$ which are G-relative H-invariant polynomials for some maximal subgroup H when G satisfies the conditions given.*

SqrtDisc, [Gei03] Algorithm 6.24 Step 1: *When $G \not\leq A_n, H < A_n$*

$$I(\underline{X}) = \prod_{1 \leq i < j \leq n} (X_i - X_j)$$

[Note that if we checked whether the discriminant was a square then this invariant gives no additional information used directly since if $G \not\leq A_n$ no even permutation group will be the Galois group and we can make that decision purely on the parity of H.]

D, [Gei03] Satz 6.8, Algorithm 6.24 Step 3.2.2: *When G is a subgroup of $S_{n/l} \wr_\Gamma S_l$ for some $l|n$, $\Gamma = \{1, \ldots, l\}$, H is a subgroup of $S_{n/l} \wr_\Gamma A_l$ having the same block systems as G,*

$$I(\underline{X}) = \prod_{1 \leq i < j \leq \#B} (y_i - y_j)$$

where $y_j = \sum_{j' \in b_j} X_{j'}$ and B is a block system of both G and H, $|B| = l, \#b_j = n/l, b_j \in B$.

s_m, [Gei03] Satz 6.8, Algorithm 6.24 Step 3.2.4: *When G is a subgroup of $S_{n/l} \wr_\Gamma S_l$ for some $l|n$, $\Gamma = \{1, \ldots, l\}$, there is a subgroup H of index 2 with the same block systems as G such that*

$$I(\underline{X}) = \prod_{b \in B} \prod_{i,j \in b, i<j} (X_j - X_i)$$

is a G-relative H-invariant polynomial, for all block systems B of both G and H, $|B| = l, \#b_i = n/l, b_i \in B$,

D s_m, [Gei03] Satz 6.8, Algorithm 6.24 Step 3.2.6: *When G is a subgroup of $S_{n/l} \wr_\Gamma S_l$ for some $l|n$, $\Gamma = \{1, \ldots, l\}$, there is a subgroup H of index 2 with the same block systems as G such that*

$$I(\underline{X}) = D(\underline{X}) \times s_m(\underline{X})$$

is a G-relative H-invariant polynomial.

s_1, [Gei03] Satz 6.8, Algorithm 6.24 Step 3.2.3: *When G is a subgroup of $S_{n/l} \wr_\Gamma S_l$ for some $l|n$, $\Gamma = \{1, \ldots, l\}$, H is a subgroup of $A_{n/l} \wr_\Gamma S_l$ with the same block systems as G,*

$$I(\underline{X}) = \sum_{b \in B} \prod_{i,j \in b, i<j} (X_i - X_j)$$

where B is a block system of both G and H, $|B| = l, \#b = n/l, b \in B$.

s_2, [Gei03] Satz 6.8, Algorithm 6.24 Step 3.2.5: *When G is a subgroup of $S_{n/l} \wr_\Gamma S_l$ for some $l|n$, $\Gamma = \{1, \ldots, l\}$, there is a subgroup H of index 2^{l-1} with the same block systems as G such that*

$$I(\underline{X}) = \sum_{b_{i_1}, b_{i_2} \in B, i_1 \neq i_2} d_{i_1} d_{i_2}$$

is a G-relative H-invariant polynomial where B is a block system of G and H, $|B| = l, \#b = n/l, b \in B$ and $d_i = \prod_{j,j' \in b_i, j<j'} (X_j - X_{j'})$.

Proof. We refer to existing proofs where possible.

SqrtDisc, [Gei03] Algorithm 6.24 Step 1: Note that the proof that this I is G-relative H-invariant follows from substituting $\bar{u} = -1$ in the SqrtDisc proof of Theorem 8.1.

D, [Gei03] Satz 6.8, Algorithm 6.24 Step 3.2.2: Since this invariant has been considered elsewhere ([**Gei03**], [**GK00**] Lemma 2.13 and [**FK14**] following Theorem 5.7) we will not prove this is an invariant. Note that this is not a G-relative H-invariant in characteristic 2, since it relies on multiplications of -1.

s_m, [Gei03] Satz 6.8, Algorithm 6.24 Step 3.2.4: See Theorem 5.7 of [**FK14**]. Note that this is not a G-relative H-invariant in characteristic 2, since it relies on multiplications of -1.

D s_m, [Gei03] Satz 6.8, Algorithm 6.24 Step 3.2.6: See [**GK00**] Lemma 2.13 and [**FK14**] following Theorem 5.7. Note that this is not a G-relative H-invariant in characteristic 2, since it relies on multiplications of -1.

s_1, [Gei03] Satz 6.8, Algorithm 6.24 Step 3.2.3: Note that this equivalent to the F invariant of Theorem 8.3 where the inner invariant F is the SqrtDisc invariant.

s_2, [Gei03] Satz 6.8, Algorithm 6.24 Step 3.2.5: As both [**Gei03**] and [**Eic96**] state this invariant we will not prove that it is an invariant. Note that this is not a G-relative H-invariant in characteristic 2 since it relies on multiplications of -1.

□

Note the order in [**Gei03**] Algorithm 6.24. The SqrtDisc, ProdSum, D, s_1, s_m, s_2 and Ds_m invariants appear first in the algorithm as these are the cheaper invariants to apply (although we may use techniques from later steps to calculate them). Although in characteristic 2 we cannot use most of them, the ones we can use are listed first in [**Gei03**] Algorithm 6.24, (Steps 1 (SqrtDisc), 3.1 (ProdSum) and 3.2.2 (D)). Note also that [**Gei03**] Algorithm 6.24 can be recursive so that some invariants are computed from the invariants of related groups. This occurs in Steps 4, 5 and 6.

We now state a theorem for combining invariants similar to Theorem 8.2.

Theorem 8.5 ([**Gei03**] Satz 6.21, Algorithm 6.24 Step 5, [**FK14**] Lemma 5.8)**.** *Let $H_1, H_2 \subset G \subseteq S_n$ be two distinct subgroups of index 2 in G with G-relative H_i-invariants I_i and $G//H_i = \{\mathrm{Id}, \tau_i\}$. Then*

$$I(\underline{X}) = I_1 I_2, \text{ if } I_i^{\tau_i} = -I_i$$

$$I(\underline{X}) = (I_1 - I_1^{\tau_1})(I_2 - I_2^{\tau_2}) \text{ otherwise}$$

is a G-relative H-invariant where $H = (H_1 \cap H_2) \cup ((G \setminus H_1) \cap (G \setminus H_2))$ when the characteristic of F is not 2.

Proof. That these $I(\underline{X})$ are G-relative H-invariants is proven in [**FK14**] Lemma 5.8. The resolvent polynomials in this case define quadratic Kummer extensions of the invariant ring $\mathbb{F}_q[t](\underline{X})^G$ instead of Artin–Schreier extensions as in Theorem 8.2. We note that negation is equivalent to the identity and subtraction is equivalent to addition in characteristic 2 hence there cannot be G-relative H_i-invariants I_1, I_2 such that $I_i^{\tau_i} = -I_i = I_i$ since any such polynomial is G-invariant and $I_i - I_i^{\tau_i} = I_i + I_i^{\tau_i}$ is G-invariant also.

□

Further combinations of invariants are possible, see [**FK14**] following Lemma 5.8.

Theorem 8.6. *The generic invariants*

$$I(\underline{X}) = \sum_{h \in H//\mathrm{Stab}_H b^\sigma} b^{\sigma h} = \sum_{m \in \mathrm{Orb}_H(b^\sigma)} m,$$

where b is a monomial and $\sigma \in S_n$ is such that $|\mathrm{Orb}_G(b^\sigma)| > |\mathrm{Orb}_H(b^\sigma)|$ or equivalently $(G : \mathrm{Stab}_G b^\sigma) \neq (H : \mathrm{Stab}_H b^\sigma)$, and

$$I(\underline{X}) = \sum_{\tau \in H} (\prod_{i=1}^{n-1} X_i^i)^\tau,$$

are G-relative H-invariant polynomials for all groups G and maximal subgroups H independent of characteristic.

See [**FK14**] Section 4 for a discussion on computing efficient monomials, also [**Gei03, GK00**].

Proof. In the first formula, for $h \in H, I^h(\underline{X}) = \sum_{m \in \mathrm{Orb}_H(b^\sigma)} m^h$, and since $h \in H, m^h \in \mathrm{Orb}_H(b^\sigma), I^h = I$. However, for $g \in G \setminus H, I^g(\underline{X}) = \sum_{m \in \mathrm{Orb}_H(b^\sigma)} m^g$, but since $g \notin H$, $|\mathrm{Orb}_G(b^\sigma)| > |\mathrm{Orb}_H(b^\sigma)|, m^g \notin \mathrm{Orb}_H(b^\sigma)$, $I^g \neq I$. This proof is independent of characteristic.

In the last formula, for $h \in H, I^h(\underline{X}) = \sum_{\tau \in H} (\prod_{i=1}^{n-1} X_i^i)^{h\tau}$, but since $h\tau \in H$, $I^h = I$. However, for $g \in G \setminus H, I^g(\underline{X}) = \sum_{\tau \in H} (\prod_{i=1}^{n-1} X_i^i)^{g\tau} = I(\underline{X})$ implies that $(\prod_{i=1}^{n-1} X_i^i)^{g\tau} = (\prod_{i=1}^{n-1} X_i^i)^h$ for some $h \in H$ and $g\tau = h$ implies that $g \in H$ – a contradiction, therefore $I^g \neq I$. This proof is independent of characteristic. □

Note that in characteristic p $\sum_{h \in H} b^{\sigma h}$ is not necessarily G-relative (but it is in characteristic 0) as we may get cancellations which make the polynomial invariant outside of H.

8.7. Tschirnhausen Transformations (Algorithm 11, Step 6(c)ii)

To use Theorem 7.4 the resolvent polynomial needs to have a root in F which is a single root. We can make this happen by applying a suitable Tschirnhausen transformation to the invariant we are using. A *Tschirnhausen transformation* is a polynomial which gives a change of variable ([**Tig01**] Section 6.4). We use Tschirnhausen transformations on all of the variables in an invariant. When F has characteristic p Tschirnhausen transformations are in $R = \mathbb{F}_q[t]$. We cannot use $R = \mathbb{F}_q$ because there may not be enough polynomials over $\mathbb{F}_q$ to ensure that the application of one of them will make a root of the resolvent in F be a single root. These transformations then need to be mapped to the chosen $E[[\rho]]$ using the map h in Section 8.2 for evaluation at the roots of f in $E[[\rho]]$ as do the invariants themselves.

8.8. Determining a Descent (Algorithm 11, Steps 6b and 6(c)vB)

We have a group G such that $\mathrm{Gal}(f) \subseteq G$ and a maximal subgroup H of G for which we are testing whether $\mathrm{Gal}(f) \subseteq H$. We have chosen a G-relative H-invariant polynomial I and a Tschirnhausen transformation T (Step 6(c)ii). Now we need to decide whether

$I^\tau(T(\alpha_1),\dots,T(\alpha_n)) \in F$ for $\tau \in G//H$, then, if $I^\tau(T(\alpha_1),\dots,T(\alpha_n)) \in F$ is a single root for some $\tau \in G//H$, it will follow from Theorem 7.4 whether $\mathrm{Gal}(f) \subseteq \tau H \tau^{-1}$.

We evaluate $I^\tau(T(s\bar{\alpha}_1),\dots,T(s\bar{\alpha}_n))$ in $E[[\rho]]$ to some precision m which we will choose and we can map this evaluation back to F/P^m using h_m^r. Here it is convienient that we use the scaled roots of f which are in the integral closure $\mathbb{Z}_F^0$ of $k[t]$ in F. Integral elements of F will have finite expansions in $E[[\rho]]$ when F is a rational function field and integral coefficients with finite expansions otherwise. Integral elements do not require denominator bounds. We can bound the image of the evaluation and we use this bound to compute a precision such that all non-zero P-adic digits of $I^\tau(T(s\alpha_1),\dots,T(s\alpha_n))$ can be computed. When F is a global function field we use a bound on the degree if F is rational or, more generally, the infinite valuations of the element. This will either prove that $\mathrm{Gal}(f) \subseteq \tau H \tau^{-1}$ (if $-v_\infty(h_{r,m}(I^\tau(T(s\bar{\alpha}_1),\dots,T(s\bar{\alpha}_n)))) \le \tilde{B}$ for all infinite valuations v_∞ of F and some bound $\tilde{B}$), suggest that this is probably true (if the previous inequality holds but we use less precision than we should) or prove that it is not true (if the inequality doesn't hold).

To compute such a bound $\tilde{B}$ we use the minimum infinite valuation of the roots of f_s. The infinite valuation of a rational function is the negative of its degree. We compute these valuations using the Newton polygons of the polynomial f_s over F at all infinite places of F and call the smallest one v_0.

Let

$$I^\tau\left(T(s\alpha_1),\dots,T(s\alpha_n)\right) = \sum_j c_j \prod_i T(s\alpha_i)^{d_{ij}}$$

(in which form any invariant can be written), remembering that the invariants may have coefficients $c_j \in F_q[t]$ and not only in $\mathbb{Z}$ as in the case when the characteristic is 0. Then

$$v_\infty\left(I^\tau(T(s\alpha_1),\dots,T(s\alpha_n))\right) \ge \min_j\{v_\infty(c_j) + \sum_i d_{ij} v_\infty(T(s\alpha_i))\}$$

but since $v_\infty(s\alpha_i) \ge v_0$ for all i and $v_\infty(T(s\alpha_i)) \ge \min_l\{v_\infty(T_l) + l v_\infty(s\alpha_i)\}$, where T_l are the non zero coefficients of T, we have

$$v_\infty\left(I^\tau(T(s\alpha_1),\dots,T(s\alpha_n))\right) \ge \min_j\{v_\infty(c_j) + \min_l\{v_\infty(T_l) + l v_0\} \sum_i d_{ij}\}.$$

But $v_0 \le 0$ (since f_s is over $\mathbb{F}_q[t]$ or more generally its integral closure $\mathbb{Z}_F^0$ in F) and $v_\infty(T_l) \le 0$ so $(v_\infty(T_l) + l v_0)\sum_i d_{ij} \le 0$ for all l, j so we use $d = \max_j\{\sum_i d_{ij}\}$ to minimize $\min_j\{v_\infty(c_j) + \min_l\{v_\infty(T_l) + l v_0\}\sum_i d_{ij}\}$. Therefore

$$v_\infty(I^\tau(T(s\alpha_1),\dots,T(s\alpha_n))) \ge \min_j\{v_\infty(c_j)\} + \min_l\{v_\infty(T_l) + l v_0\} d$$

since $v_\infty(c_j) \leq 0$ also and when F is a rational function field

$$\begin{aligned}\deg(I^\tau(T(s\alpha_1),\ldots,T(s\alpha_n))) &= -v_\infty(I^\tau(T(s\alpha_1),\ldots,T(s\alpha_n))) \\ &\leq \max_j\{-v_\infty(c_j)\} + \max_l\{-v_\infty(T_l) - lv_0\}d.\end{aligned}$$

When F is an algebraic function field there is possibly more than one infinite place. The minimum infinite valuation v_0 is taken as the minimum over all infinite places. We have the bound $-v_\infty(I^\tau(T(s\alpha_1),\ldots,T(s\alpha_n))) \leq \max_j\{-v_\infty(c_j)\} + \max_l\{-v_\infty(T_l) - lv_0\}d$ where this holds for all infinite valuations v_∞.

In practice the $d = \deg(I)$ we use in this multiplication may be larger than $\max_j\{\sum_i d_{ij}\}$ because we compute the degree of an unreduced invariant, so this will cost us in using more precision than necessary but will not decrease the accuracy of the result.

Therefore if F is a rational function field and $I^\tau(T(s\alpha_1),\ldots,T(s\alpha_n))$ is a polynomial we have a bound on the degree of the polynomial and if F is an algebraic function field and $I^\tau(T(s\alpha_1),\ldots,T(s\alpha_n)) \in \mathbb{Z}_F^0$ we have a bound on its infinite valuations. However, if $I^\tau(T(s\alpha_1),\ldots,T(s\alpha_n))$ does not satisfy these bounds then it is either not polynomial or not an element of $\mathbb{Z}_F^0$ and there is no descent into $\tau H\tau^{-1}$.

8.8.1. Precision (Algorithm 11, Step 6(c)iii). Let $\beta = I(T(s\alpha_1),\ldots,T(s\alpha_n))$ whose infinite valuations are bounded below by $-B$ if $\beta \in \mathbb{Z}_F^0$ where

$$B = \deg(I)\max_{0\leq l\leq \deg(T)}\{-v_0 l - \max_{v_\infty}\{v_\infty(T_l)\}\} + \max_{j,v_\infty}\{-v_\infty(c_j)\}$$

where T_l are the coefficients of T, c_j are the coefficients of I and let $\beta \in \beta_0 + P^m$ for some precision m, that is, β_0 is an approximation to β. To determine whether β is a finite expansion and so an element of $\mathbb{Z}_F^0$ we need to compute m which ensures that $\beta - \beta_0 = 0$ if so. For all infinite valuations v_∞ we have $-v_\infty(\beta) \leq B, -v_\infty(\beta_0) \leq B$ and $-v_\infty(\beta^{(i)}) \leq B$ for all conjugates $\beta^{(i)}$ of β, so $-v_\infty(\beta - \beta_0) \leq B$ and $-v_\infty((\beta-\beta_0)^{(i)}) \leq B$. Therefore

$$\begin{aligned}-v_\infty(\mathrm{norm}(\beta-\beta_0)) &= -v_\infty\left(\prod_i(\beta-\beta_0)^{(i)}\right) \\ &= \sum_i -v_\infty((\beta-\beta_0)^{(i)}) \\ &\leq \sum_i B \\ &\leq [G:H]B\end{aligned}$$

where the number of conjugates is the degree of the smallest normal subfield of the splitting field of f containing β. This is less than $[G : H]$ because β is in the field extension of F fixed by automorphisms in H by definition and F is a field fixed by automorphisms in G since $\mathrm{Gal}(f) \subset G$. Since $\beta - \beta_0 \in P^m$, $\mathrm{norm}(\beta - \beta_0) \in P^m$. We have $\deg((\beta - \beta_0)_0) = \deg((\beta - \beta_0)_\infty)$ so

$$\sum_{Q \in \mathbb{P}_F^0} v_Q(\beta - \beta_0) \deg(Q) = \sum_{Q \in \mathbb{P}_F^\infty} -v_Q(\beta - \beta_0) \deg(Q)$$

and

$$\begin{aligned} m \deg(P) \leq v_P(\beta - \beta_0) \deg(P) &\leq \sum_{Q \in \mathbb{P}_F^\infty} -v_Q(\beta - \beta_0) \deg(Q) \\ &\leq \sum_{Q \in \mathbb{P}_F^\infty} -v_Q(\mathrm{norm}(\beta - \beta_0)) \deg(Q) \\ &\leq \#\mathbb{P}_F^\infty \max_{Q \in \mathbb{P}_F^\infty} \{-v_Q(\mathrm{norm}(\beta - \beta_0))\} \max_{Q \in \mathbb{P}_F^\infty} \{\deg(Q)\} \\ &\leq \#\mathbb{P}_F^\infty [G : H] B \max_{Q \in \mathbb{P}_F^\infty} \{\deg(Q)\} \end{aligned}$$

and we must choose m such that

$$m > \max_{Q \in \mathbb{P}_F^\infty} \{\deg(Q)\} \#\mathbb{P}_F^\infty [G : H] B / \deg(P)$$

so that we can decide whether $\beta - \beta_0 = 0$. If F is a rational function field the above can be expressed more simply as

$$m \deg(P) = \deg(\mathrm{norm}(P^m)) \leq \deg(\mathrm{norm}(\beta - \beta_0)) = -v_\infty(\mathrm{norm}(\beta - \beta_0)) \leq [G : H] B$$

so $m > [G : H] B / \deg(P)$ is enough precision to ensure we can determine whether β is a finite expansion.

But this means that $m \sim [G : H]$ which can be quite large. Such a precision m will prove whether or not $\mathrm{Gal}(f) \subseteq H$ but we only want to use this proven precision if it is not too large, otherwise we can prove this descent step later (if necessary) using absolute resolvents as done in [**GK00**] Algorithm 5.1. If $[G : H]$ is large we instead use lB where l is some limit we place on the index $[G : H]$. Since it is most likely that $\mathrm{Gal}(f) \not\subseteq H$, the limit l will give us a smaller precision which may allow us to determine that $\mathrm{Gal}(f) \not\subseteq H$. We use a precision of $(\lceil \max_{Q \in \mathbb{P}_F^\infty} \{\deg(Q)\} \#\mathbb{P}_F^\infty lB / \deg(P) \rceil + \epsilon)$ to allow us to check that

the few digits above where we expect the series expansion in a uniformizing element of P of an exact root to finish are zero.

While this bound for m gives us a precision which proves the descent we can also use a lower precision to detect possible descents and only use m greater than this bound for those $\tau \in G//H$ for which we have not ruled out at a lower precision that a descent is possible. An expansion may have a large number of zero digits in the middle before non zero digits of high powers of the uniformizing element of P. In this case a lower precision will detect that a descent is possible but the larger precision will prove whether this descent is correct. A descent is only proven if a root is proven to be in F.

8.9. Examples

The timings given in this section are for computations on an Intel(R) Core(TM) i7-3770 CPU 3.4GHz (32GB RAM) using Magma V2.19-9.

We identify transitive groups in the form dTn, the nth transitive group of degree $d \leq 32$ according to the ordering in the database of transitive groups in Magma [**CBFS10**]. This is the same numbering used in GAP [**GG02**] when $d < 32$ where the groups have been either confirmed or provided by Hulpke [**Hul05**]. The transitive groups of degree 32 were provided by [**CH08**].

Example 12. *Let $p = 7, F = \mathbb{F}_7(t)$ and $f = x^8 + t + 1$ over F. The field $F[x]/f$ has 2 proper subfields of degrees 4 and 2 which are both generating subfields. Using the Galois groups of these subfields, we compute $8T26$ as a starting group which has order 64. This starting group has 6 conjugacy classes of transitive maximal subgroups, however only 2 of them contain the cycle shapes computed when choosing the prime $t^2 + 2$ from which we computed $\mathbb{F}_{7^{16}}[[z]]$ over which f splits. We first attempt to compute a descent to $8T15$. Using a BlockQuotient invariant from Theorem 8.3 we find we need to transform by a Tschirnhausen transformation. However this is too expensive so instead we attempt a descent to another subgroup conjugate to $8T15$ in S_8. Here we use an invariant computed by applying Theorem 8.5 and again we need to apply a Tschirnhausen transformation. Instead we return to the attempt on the first subgroup and after applying a few transformations we decide not to descend into this subgroup. Moving back to the other possible conjugacy class of subgroups, which are also conjugate to $8T15$ in S_8, we transform once before we decide that the Galois group of f is contained in this conjugacy class of subgroups of order 16.*

Now we compute the maximal subgroups of $8T15$ of which there are 6 transitive conjugacy classes but we need only consider 4. We first attempt descents using generic invariants

into 2 subgroups conjugate to $8T6$ *in* S_8 *but after applying several transformations we move on to attempting a descent into* $8T8$*. After applying a Tschirnhausen transformation to a generic invariant we attempt a descent into one conjugate of* $8T6$ *in* S_8 *using a generic invariant and decide not to descend. We make several more attempts with transformations and a generic invariant to descend into the first subgroup and decide that the first subgroup conjugate to* $8T6$ *which we attempted contains the Galois group of* f*. This group has 2 classes of transitive maximal subgroups however neither of them contain the cycle shapes so there are no more subgroups to consider and the Galois group of* f *is* $8T6$*.*

This computation took 0.38s.

We move on to some examples in characteristic 2.

Example 13. *Let* $p = 2, F = \mathbb{F}_2(t)$ *and* $f = x^5+x^4+tx^3+x+1$ *or* $f = x^8+x^7+tx^6+x^5+x^2+tx+1$*. In both of these simple examples there are subgroups of* S_n *but none of them need consideration for a descent because either the subgroups are not transitive or the cycle structure of the group is not contained in the information we have about the cycle structure of the Galois group from the computation of the prime. Therefore the Galois groups of these polynomials are* S_5 *and* S_8 *respectively.*

Example 14. *Let* $p = 2, F = \mathbb{F}_2(t)$ *and* $f = x^8 + x^4 + x - t$ *over* F*. The field* $F[x]/f$ *has no proper subfields so we start descending from* S_8 *which has 4 conjugacy classes of transitive maximal subgroups, 2 of which contain the cycle shapes computed when choosing the prime* t^2+t+1 *from which we computed* $\mathbb{F}_{2^{14}}[[z]]$ *over which* f *splits. We first attempt to compute a descent to* $8T49$ *using a SqrtDisc invariant from Theorem 8.1 since this class of subgroups contains* A_n *and immediately gain a descent. This subgroup has 3 classes of transitive maximal subgroups, only 2 which we need consider. Using a generic invariant we gain a descent to a class conjugate to* $8T48$ *which has 4 classes of transitive maximal subgroups, 2 of which we consider. We attempt a descent into* $8T37$ *but find we need to apply a transformation to the generic invariant used and after doing so decide the Galois group is not contained in* $8T37$*. We decide that the Galois group is contained in* $8T36$ *after using a transformation with another generic invariant. This subgroup has 2 classes of transitive maximal subgroups, only 1 which is worth considering. Several transformations on a generic invariant later we decide that the Galois group is contained in* $8T25$ *which has one class of transitive maximal subgroups which we do not consider because the cycle structure of the subgroups is not contained in the information we have about the cycle*

structure of the Galois group from the computation of the prime, hence $8T25$ *is the Galois group of* f.

This computation took 0.19s.

Example 15. *Let* $p = 2, F = \mathbb{F}_2(t)$ *and* $f = x^9 + (t^6+t^3+1)x^7 + (t^9+t^8+t^5+t^2+1)x^5 + (t^{11}+t^{10}+t^2+t)x^4 + (t^{14}+t^{13}+t^{11}+t^8+t^7+t)x^3 + (t^{15}+t^{14}+t^{13}+t^{12}+t^9+t^7+t^5+t)x^2 + (t^{15}+t^{14}+t^{12}+t^{11}+t^{10}+t^5+t^2+t+1)x + t^{14}+t^{13}+t^{12}+t^{11}+t^{10}+t^6+t^5+t^4+t^2+t+1$ *over* F [**KM**]. *The field* $F[x]/f$ *has 1 generating subfield of degree* 3 *from which we compute a starting group as* $9T31$ *which has 4 classes of transitive subgroups. We first consider the class of* $9T28$ *using a D invariant from Theorem 8.1. After applying a Tschirnhausen transformation we decide that the Galois group is contained in this class of subgroups which themselves have 2 subgroups. Using a BlockQuotient invariant from Theorem 8.3 and a transformation we decide that the Galois group is contained in* $9T22$ *which has only one class of transitive subgroups containing the cycle shapes computed when choosing the prime* t^2+t+1 *from which we computed* $\mathbb{F}_{2^{18}}[[z]]$ *over which* f *splits. With the class of subgroups* $9T17$ *we use a SqrtDisc invariant from Theorem 8.1 to decide that it does contain the Galois group. Now there are 2 classes of subgroups to consider, both conjugate to* $9T6$ *in* S_9 *and we attempt a descent with a generic invariant which fails, however the descent into the other class also with a generic invariant succeeds. Next we attempt descents to 3 classes of subgroups conjugate to* $9T1$ *in* S_9 *and after applying a Tschirnhausen transformation to one of these we gain a descent. This group has no transitive subgroups so it must be the Galois group of* f *over* F.

This computation took 0.79s.

Example 16. *In Tables 8.1 to 8.8 we summarise the subgroups and invariants used in the descent of the computation of Galois groups of some polynomials mostly from Klüners and Malle* [**KM**] *or polynomials defining subfields of the fields defined by these polynomials.*

When there are 2 or more classes of subgroups which are conjugate in S_n *and we use the same invariant for 2 or more of these classes we do not list the subgroup class and invariant twice consecutively but note the number of such conjugate classes for which we attempt a descent in "No. classes attempted". The entry in the "Successful" column means that we were successful in a descent into one of these classes.*

Note that it is possible that a descent will not be decided since another attempt after a transformation may have become more expensive than attempting a descent for another subgroup. A descent on a cheaper subgroup will first be attempted and if this fails or becomes

more expensive we may return to continue to attempt a descent on a subgroup we had not decided on, hence some subgroups may appear more than once in the list of "Subgroup Class".

$F = \mathbb{F}_2(t)$	$f = x^{10} + tx^7 + (t^2+t)x^5 + tx^4 + tx^3 + (t^2+1)x^2 + (t^2+t)x + t$			
Prime : $t^2 + t + 1$	*Splits over :* $\mathbb{F}_{2^{20}}[[z]]$			
Subgroup Class	*No. classes attempted*	*Invariant Type*	*Successful*	*Time*
$10T43$	-	*Subfields*	-	
$10T41$	*1*	*Factor Delta* [**Els14b**]	*Yes*	
$10T22$	*2*	*Theorem 8.3 ProdSum*	*No*	
$10T27$	*1*	*Theorem 8.3 F*	*Yes*	
$10T17$	*2*	*Theorem 8.3 BlockQuotient*	*No*	
$10T19$	*1*	*Theorem 8.3 BlockQuotient*	*Yes*	*0.57s*

Table 8.1

$F = \mathbb{F}_2(t)$	$f = x^6 + x^5 + x^4 + x^3 + (t^2+t+1)x^2 + (t^2+t+1)x + t^2 + t + 1$			
Prime : $t^3 + t^2 + 1$	*Splits over :* $\mathbb{F}_{2^9}[[z]]$			
Subgroup Class	*No. classes attempted*	*Invariant Type*	*Successful*	*Time*
$6T11$	-	*Subfields*	-	
$6T6$	*1*	*Theorem 8.1 D*	*undecided*	
$6T3$	*1*	*Theorem 8.3 ProdSum*	*No*	
$6T8$	*1*	*FactorDelta* [**Els14b**]	*undecided*	
$6T6$	*1*	*Theorem 8.1 D*	*Yes*	
$6T4$	*1*	*Theorem 8.1 SqrtDisc*	*Yes*	*0.18s*

Table 8.2. [**Els13b**]

8.10. Timings

The computations we give timings for in this section were run on an Intel(R) Core(TM) i7-3770 CPU 3.4GHz (32GB RAM) using Magma V2.19-9.

$F = \mathbb{F}_2(t)$	$f = x^{15} + t^2x^{11} + x^{10} + tx^8 + t^4x^7 + x^5 + t^6x^3 + t^4x^2 + t^5$			
Prime : $t^2 + t + 1$	*Splits over :* $\mathbb{F}_{2^{10}}[[z]]$			
Subgroup Class	*No. classes attempted*	*Invariant Type*	*Successful*	*Time*
$15T93$	-	*Subfields*	-	
$15T87$	*1*	*Theorem 8.3 E*	*No*	
$15T83$	*1*	*Theorem 8.3 BlockQuotient*	*Yes*	
$15T70$	*1*	*Block Transfer* [**Els14b**]	*Yes*	
$15T52$	*1*	*Theorem 8.3 E*	*No*	
$15T62$	*1*	*Theorem 8.1 SqrtDisc*	*Yes*	
$15T42$	*1*	*Theorem 8.3 E*	*No*	
$15T10$	*2*	*Generic*	*Yes*	*1.58s*

Table 8.3

$F = \mathbb{F}_{2^2}(t)$	$f = x^{12} + x^9 + x^8 + x^6 + x^4 + x^3 + x^2 + x + t + 1$			
Prime : $t^3 + wt^2 + w^2t + w, \mathbb{F}_{2^2} = \mathbb{F}_2\langle w\rangle$		*Splits over :* $\mathbb{F}_{2^{36}}[[z]]$		
Subgroup Class	*No. classes attempted*	*Invariant Type*	*Successful*	*Time*
$12T56$	-	*Subfields*	-	
$12T7$	*2*	*Theorem 8.3 ProdSum*	*undecided*	
$12T6$	*2*	*Generic*	*undecided*	
$12T7$	*2*	*Theorem 8.3 ProdSum*	*undecided*	
$12T6$	*1*	*Generic*	*undecided*	
$12T7$	*2*	*Theorem 8.3 ProdSum*	*undecided*	
$12T6$	*1*	*Generic*	*undecided*	
$12T7$	*2*	*Theorem 8.3 ProdSum*	*No*	
$12T6$	*2*	*Generic*	*Yes*	*0.82s*

Table 8.4

In Table 8.9 are average times and minimum and maximum times where they differ substantially, for the computations of Galois groups of 5 random monic additive polynomials over $\mathbb{F}_p[t]$ of degree p^d. We have used additive polynomials for these timings since we know the result of the Galois group computation is not S_n.

The polynomials for which we can compute a Galois group in some reasonable time are restricted by the Subfields algorithm which factors the polynomial over the field it defines,

$F = \mathbb{F}_{29}(t)$	$f = x^4 + 26x^3 + (4t^2 + 28)x^2 + (6t^2 + 17)x + 4t^4 + 13t^2 + 16$			
Prime : $t^2 + 2$	*Splits over :* $\mathbb{F}_{29^2}[[z]]$			
Subgroup Class	*No. classes attempted*	*Invariant Type*	*Successful*	*Time*
$4T3$	-	*Subfields*	-	
$4T1$	*1*	*Theorem 8.4 DSm*	*No*	
$4T2$	*1*	*Theorem 8.4 SqrtDisc*	*No*	*0.14s*

TABLE 8.5

$F = \mathbb{F}_{29}(t)$	$f = x^{12} + 4x^{10} + 4tx^9 + 21x^8 + tx^7 + (15t^2 + 13)x^6 + 7tx^5 + (13t^2 + 24)x^4 + (26t^3 + 2t)x^3 + (11t^2 + 21)x^2 + (10t^3 + 21t)x + 4t^2 + 10$			
Prime : $t^2 + 2$	*Splits over :* $\mathbb{F}_{29^2}[[z]]$			
Subgroup Class	*No. classes attempted*	*Invariant Type*	*Successful*	*Time*
$12T292$	-	*Subfields*	-	
$12T273$	*1*	*Theorem 8.4* s_2	*Yes*	
$12T253$	*1*	*Theorem 8.3 BlockQuotient*	*Yes*	
$12T205$	*1*	*Theorem 8.3 BlockQuotient*	*Yes*	
$12T142$	*1*	*Theorem 8.3 ProdSum*	*No*	
$12T45$	*1*	*Theorem 8.3 ProdSum*	*No*	
$12T129$	*1*	*Generic*	*Yes*	
$12T59$	*1*	*Theorem 8.3 ProdSum*	*No*	
$12T85$	*1*	*Theorem 8.4 SqrtDisc*	*No*	*0.46s*

TABLE 8.6

unless it can be determined using the cycle information that the field has no subfields. This is why we do not report a time for $p = 11, d = 2$ in Table 8.9.

$F = \mathbb{F}_{29}(t)$	$f = x^{12} + 26tx^8 + 13t^2x^6 + 20t^2x^4 + 27t^3$			
Prime : $t^2 + 13t + 21$	*Splits over :* $\mathbb{F}_{29^8}[[z]]$			
Subgroup Class	*No. classes attempted*	*Invariant Type*	*Successful*	*Time*
$12T227$	-	*Subfields*	-	
$12T137$	*1*	*Theorem 8.3 BlockQuotient*	*Yes*	
$12T111$	*2*	*Generic*	*undecided*	
$12T110$	*1*	*Theorem 8.5*	*undecided*	
$12T111$	*1*	*Generic*	*undecided*	
$12T110$	*2*	*Theorem 8.5*	*undecided*	
$12T111$	*2*	*Generic*	*No*	
$12T110$	*2*	*Theorem 8.5*	*No, Yes*	*2.22s*

Table 8.7

$F = \mathbb{F}_{29}(t)$	$f = x^{12} + 15x^{10} + 16x^9 + 3x^8 + 4x^7 + (19t + 9)x^6 + (26t + 9)x^5 + (25t + 7)x^4 + 21tx^3 + 20tx^2 + 12tx + 3t$			
Prime : $t^2 + 15t + 9$	*Splits over :* $\mathbb{F}_{29^6}[[z]]$			
Subgroup Class	*No. classes attempted*	*Invariant Type*	*Successful*	*Time*
$12T136$	-	*Subfields*	-	
$12T108$	*2*	*Theorem 8.3 F*	*undecided, No*	
$12T109$	*2*	*Theorem 8.3 F*	*undecided, No*	
$12T108$	*1*	*Theorem 8.3 F*	*No*	
$12T109$	*1*	*Theorem 8.3 F*	*Yes*	*0.52s*

Table 8.8

	$p = 2$					$p = 3$		
d	1	2	3	4	5	1	2	3
Average time	0.014s	0.008s	0.058s	0.47s	131.72s	0.016s	0.108s	6.936s
Min/Max time					33s/490s			2s/22s

	$p = 5$		$p = 7$		$p = 11$		$p = 29$
d	1	2	1	2	1	2	1
Average time	0.032s	7.866s	1.762s	533.104s	0.662s	-	57.360s
Min/Max time		2s/24s		350s/1210s			7s/122s

Table 8.9

Chapter 9

Galois Groups of Reducible Polynomials

9.1. An Algorithm for Reducible Polynomials

Since Galois groups describe relationships between the roots of a polynomial we can also compute Galois groups of reducible polynomials in a similar way to those of irreducible polynomials. Magma [**CBFS10**] has contained an implementation of an algorithm for Galois groups of reducible polynomials over $\mathbb{Q}$ since V2.13. This has since been extended to accept input of reducible polynomials over number fields (V2.17) and reducible polynomials over global rational and algebraic function fields (V2.18).

The algorithm we give for Galois groups of reducible polynomials extends Algorithm 11 as we factorize the input polynomial and use the product of the Galois groups of the factors as a group in which we know the Galois group of the product is contained. We need to make sure the place chosen is good for all factors of the input polynomial and that we compute a completion which contains all roots of all factors of the input. Note that since the Galois group of a reducible polynomial is a subgroup of a direct product of permutation groups it will be intransitive and each root will only be mapped by F-automorphisms to other roots of the irreducible factor it is a root of.

Algorithm 12 (Compute the Galois Group of a reducible polynomial f)**.**
Input:

- *A polynomial f over a number field F (including $\mathbb{Q}$) or global function field F (rational or algebraic), whose factors are separable.*

Output:

- *The Galois group of f.*

Steps:

1. *Factorize f over F as $\prod_i f_i^{e_i}$ and compute the squarefree product $\tilde{f} = \prod_{\{i:\deg(f_i)>1\}} f_i$ of the non-linear factors (without multiplicities).*
2. *Choose a finite place P such that the image of $\tilde{f}$ is also squarefree over the residue field at P.*

3. *Compute the Galois group G_1 of f_1 using Algorithm 11.*
4. *Compute the splitting field $S_{f,P}$ for f over the completion of F at P as an extension of $S_{f_1,P}$ where $S_{f_1,P}$ is the splitting field for f_1 over the completion of F at P used in the computation of G_1.*
5. *Compute the Galois groups G_i of the remaining non-linear f_i using Algorithm 11 and roots of f in the splitting field $S_{f,P}$. The Galois group G_i will be S_1 when f_i is linear.*
6. *Divide the factors f_i into 2 groups – one containing those factors for which we can easily check that the splitting field S_{f_i} intersects with the splitting field of the product of the other factors in F only and one containing the other factors. Compute the direct product $G = \oplus G_i$ for the factors f_i in this second group.*
7. *Apply Algorithm 11 Step 5 to compute the Galois group G' of the product of the factors in the second group by descent from G.*
8. *Compute the direct product $\oplus G_i \oplus G'$ for the groups G_i corresponding to factors f_i in the first group in Step 6 and map this to a subgroup of the direct product of all G_i which is the Galois group of $\tilde{f}, G_{\tilde{f}}$.*
9. *Handle multiple and linear factors by computing the image of $G_{\tilde{f}}$ under the embedding*

$$G_{\tilde{f}} \to G_{\tilde{f}} \bigoplus_{f_i \text{ not linear}} G_i^{e_i-1} \bigoplus_{f_i \text{ linear}} S_1^{e_i} \tag{5}$$

which maps a generator of $G_{\tilde{f}}$ to the product of its projections onto each addend, to gain $\mathrm{Gal}(f)$. *Return $Gal(f)$.*

9.2. Details of the Algorithm

Here we detail the steps of Algorithm 12 for Galois groups of reducible polynomials, considering especially its implementation for polynomials over a function field of characteristic p. We will attempt to describe the details as generally as possible and will note when the details we give are specific to F being a global function field.

9.2.1. Choosing a Good Place (Algorithm 12, Step 2). Most of Section 8.1 holds when f is a reducible polynomial. However we cannot determine whether the Galois group is S_n or A_n by looking at the cycle lengths. In fact the Galois group of a reducible polynomial will not be S_n or A_n as the Galois group is not transitive because the polynomial is not irreducible [**DS00**]. We choose our place with the smallest $r_P d_P l_{f,P}^{1.5} > n_i/4$ for all n_i, where n_i is the degree of f_i and $l_{f,P}$ is the number of factors of f mod P, if such a place

occurs in those we have considered otherwise a place we considered with largest $r_P d_P l_{f,P}^{1.5}$. This makes the place as good as possible for the computation of the Galois groups of each factor f_i.

9.2.2. Computing Roots in the Splitting Field over the Completion (Algorithm 12, Step 4). We compute the splitting field $S_{f_1,P}$ of f_1 over the completion of F at P using Section 8.2. We then extend this splitting field to include the roots of the other f_i. There is a map $h_1 : F \to S_{f_1,P}$ as described in Section 8.2 which we use to map $\tilde{f}$ from a polynomial over F to a polynomial over $S_{f_1,P}$. The splitting field $S_{f,P}$ for f is then computed by factoring f over $S_{f_1,P}$ and extending the field until it includes all the roots of f. The map $h : F \to S_{f,P}$ is then given as a composition $h : F \to S_{f_1,P} \hookrightarrow S_{f,P}, h = \iota \circ h_1$ where ι is the inclusion map $\iota : S_{f_1,P} \hookrightarrow S_{f,P}$.

9.2.3. Check Disjointness of Splitting Fields (Algorithm 12, Steps 6 and 8). If the splitting fields S_{f_i} of the factors f_i overlap with the splitting fields

$$\bar{S}_{f_i} = S_{\prod_{j \neq i} f_j}$$

of the products of the other factors only in F then the Galois group of the product will be the direct product of the Galois groups of the factors, (as noted in the Restrictions at beginning of [**Sta73**]). We therefore attempt to divide our factors into 2 groups – those for which we can easily determine that S_{f_i} does not overlap with $\bar{S}_{f_i}$ and those for which we cannot easily determine this.

Since the orders of the Galois groups are the degrees of the splitting fields we first check whether the orders of the Galois groups G_i of the f_i are pairwise coprime. For those G_i whose order is coprime to that of all others, the degrees of the splitting fields S_{f_i} are pairwise coprime, hence the degrees of S_{f_i} and $\bar{S}_{f_i}$ are coprime so there can be no overlap between the splitting fields S_{f_i} and $\bar{S}_{f_i}$ outside of F and so the Galois group of the product of the corresponding f_i is the direct product of those G_i. For those factors f_i whose Galois group orders are not pairwise coprime we continue to check. Note that we can only use the remainder of this check when we know something about the ramification of extensions of F. This occurs when F is $\mathbb{Q}$ or a rational function field.

If F is $\mathbb{Q}$ we check whether the discriminants of the remaining f_i are pairwise coprime. If they are then the splitting fields S_{f_i} must overlap with the $\bar{S}_{f_i}$ in an unramified extension, of which $\mathbb{Q}$ has none non-trivial. Therefore the Galois group of the product of those f_i with coprime discriminants is the direct product of their Galois groups G_i (rather than a subgroup of).

If F is a rational function field then any constant field extension will be unramified ([**Sti93**] Theorem III.6.3) and any separable extension which does not extend the constant field will be ramified ([**Sti93**] Corollary III.5.8). To obtain information from the discriminants as when $F = \mathbb{Q}$ we also ensure that the intersection of S_{f_i} and $\bar{S}_{f_i}$ does not contain a constant field extension, that is, the intersection is ramified. We can easily check whether the stem fields $F[y]/f_i$ contain a constant field extension. Let the degree of the constant field extension in S_{f_i} be c_i. The constant field extension contained in $\bar{S}_{f_i}$ has degree $\bar{c}_i = \text{lcm}(\{c_j\}_{j \neq i})$. These two constant field extensions meet only in the coefficient ring of F if $\gcd(c_i, \bar{c}_i) = 1$ which is the same as checking whether the c_i are pairwise coprime.

We first check for pairwise coprime discriminants. For those factors f_i whose Galois groups G_i have order not coprime to some other group we collect those whose discriminants are pairwise coprime to those of all other factors we are still checking, (the factors which have non coprime discriminants we cannot determine non-overlap easily). For these factors we check whether it is possible for there to be an unramified extension in the splitting field. We first check whether the dimensions of the exact constant fields of the $F[x]/f_i$ are pairwise coprime. For those factors for which this holds we compute normal subgroups of the G_i and for those subgroups whose quotient is cyclic, we compute the fixed fields of these subgroups and check whether the LCMs of the dimensions of the exact constant fields of these fixed fields are pairwise coprime, these fixed fields contain the possible constant field extensions. If we determine that the intersection of splitting fields S_{f_i} and $\bar{S}_{f_i}$ does not extend the constant field of F (that is, the intersection is a ramified extension of F) and that the discriminant of f_i is pairwise coprime to those of other factors still being considered (the intersection is unramified) then the intersection must be a trivial extension of F, that is F itself.

Now we have divided our factors into 2 groups. We take the direct product of the G_i corresponding to the factors whose splitting fields S_{f_i} *may* intersect in a non-trivial extension of F with $\bar{S}_{f_i}$ and we compute a descent (Step 7) from this direct product only. We take the direct product of the result of this descent with the direct product of those G_i corresponding to the factors for which we could determine that the splitting fields S_{f_i} overlap with $\bar{S}_{f_i}$ in F only as the Galois group of the polynomial $\tilde{f}$.

9.2.4. Invariants (Algorithm 12, Step 7). There is an invariant given in Theorem 8.3 which may be able to be used when $H \subset G$ are intransitive groups (independent of characteristic), however we do not satisfy the additional conditions to use this invariant directly during this descent. When all the orbits of H are invariant under G we compute

the actions of G and H on the orbits of G. If this action is not the same for some orbit we compute an invariant for these actions (dependent on characteristic) and evaluate this at the appropriate X_i ([**Els14b**]). Otherwise we can map to the transitive representation of G, independent of characteristic, for details see [**FK14**] Section 6.

9.2.5. Determination (Algorithm 12, Step 7). To determine whether a G-relative H-invariant I satisfies $I^\tau(\alpha_1, \ldots, \alpha_{\bar{n}}) \in F$ for for groups $H \subset G$ we use Section 8.8 but we need to ensure that v_0 is the minimum infinite valuation of all the scaled roots of f not just the roots corresponding to any one factor of f. The computation of the precision necessary is still

$$[G : H]B/\deg(P), \text{ or } \max_{Q \in \mathbb{P}_F^\infty}\{\deg(Q)\}[G : H]B\#\mathbb{P}_F^\infty/\deg(P)$$

when F is a global function field (rational or algebraic respectively), where B is the bound for the evaluation of the invariant I at all scaled roots of f. As in Section 8.8 we can replace $[G : H]$ when it is very large by some smaller value l and attempt an unproven descent which can be proven later if it succeeds.

As noted in [**FK14**] Section 7.5, the final Galois group will be a subdirect product of the G_i so only such subgroups need to be considered.

9.2.6. Multiple and Linear Factors (Algorithm 12, Step 9). In the process of computing the Galois group one computes the roots of the polynomial in the splitting field chosen. When the polynomial has linear factors or multiple roots such roots will not have been "computed" in the computation of the Galois group, however they can easily be accounted for. The Galois group is adjusted to ensure it acts on all the roots of f by mapping it to a subgroup of the direct product (5) given in Algorithm 12 Step 9.

9.3. Examples

Example 17. *Let* $F = \mathbb{F}_{101}(t), f = (x^2 + x + 3t)^5(x^5 + 5t)(x^7 + 7t)((x + 1)^7 + 7t)$. *The first 2 factors of* f *have splitting fields* S_{f_i} *which overlap with the splitting fields of the products of the other factors,* $\bar{S}_{f_i}$, *in* F *only. The last factor has a root in the splitting field of the second last factor so the overlap of their splitting fields will be larger than* F *and a descent will be required but not from the whole direct product of the 4 Galois groups of the factors. We compute the Galois groups* $2T1, 5T1, 7T4$ *and* $7T4$ *of the factors of* f *using prime* $t^2 + 35t + 77$ *and field* $F_{101^6}[[z]]$ *over which* f *splits. The order of the Galois group of the second factor is coprime to the orders of the other groups so* $5T1$ *does not need to*

be included in the direct product to descend from. By checking discriminants we discover the overlap in the splitting fields of the 3rd and 4th factors so their Galois groups will need to be included in the direct product we descend from. We continue to check whether S_{f_1} *overlaps with* $S_{f_3 f_4}$ *outside of* F*. The discriminant of the first factor is coprime to those of the third and fourth factors and the dimension of the exact constant field of* $F[x]/f_1$ *is coprime to the dimensions of the exact constant fields of* $F[x]/f_3$ *and* $F[x]/f_4$*. The Galois group of the first factor has a cyclic subgroup and the order of that cyclic subgroup is not coprime to the orders of the cyclic subgroups of the Galois groups of the third and fourth factors so we compute the fixed fields of the quotients of the Galois groups of the first, third and fourth factors by their normal subgroups where that quotient is cyclic. We compute the exact constant fields of these fixed fields and check whether their dimensions are coprime as well as the orders of the normal subgroups. Here we find that the dimension for the first factor is coprime to that of the third and fourth factors, (the dimension for the first factor is 1), hence the Galois group of the first factor does not need to be included in the direct product we descend from.*

So we descend from the direct product of the third and fourth factors. This direct product of order 1764 has 9 subgroups, 3 of which are subdirect products of G_3 *and* G_4*. We attempt descents to 2 subgroups of index* 3*, order* 588*, using an invariant which is a more general combination than Theorem 8.5, (see* [**FK14**] *following Lemma 5.8) and an invariant gained by mapping to the transitive representation of the subgroup. We apply transformations for both subgroups but none of these attempts succeed. We attempt a descent into a subgroup of index* 2*, order* 882*, using a Factor Delta invariant from* [**Els14b**] *and this succeeds immediately. This subgroup has 7 subgroups of which 2 are subdirect products of* G_3 *and* G_4*. We again use an invariant from the transitive representation for this subgroup of order* 294 *and this descent succeeds after applying transformations. Now there are 6 subgroups out of 10 which are subdirect products and we attempt descents to all 6 subgroups of order* 42 *using invariants from the transitive representation. After applying several transformations to the invariants for 4 of these groups we have 4 failed descents but for one of the other subgroups the descent succeeds after applying several transformations. This subgroup has 3 subgroups but since none of these are subdirect products of* G_3 *and* G_4 *the descent is finished.*

We take the direct product of the Galois groups of the first 2 factors and the result of the descent as the Galois group of f *which has order* 420*. We then map this permutation group*

acting on a set of cardinality 21 *and map it onto a group acting on a set of cardinality* 29*, also with order* 420*, to account for the multiplicity of the quadratic factor of* f*.*

This computation took 1.41s on an Intel(R) Core(TM) i7-3770 CPU 3.4GHz (32GB RAM) using Magma *V2.19-10.*

9.4. Timings

In Table 9.1 are average times for the computations of Galois groups of 5 products of 2 random additive polynomials with the evaluation of one of these at $x + 1$. At least two factors of each polynomial are of degree p^d and the remaining factor is of degree p^{d-1} when $d \neq 1$. The factors were chosen with the intention that one factor (of degree p^{d-1}) would have splitting field disjoint from the splitting field of the product of the other two factors which would have splitting fields which are not disjoint. Therefore the descent will mostly be from the direct product of the Galois groups of the two degree p^d factors. The computations were run on an Intel(R) Core(TM) i7-3770 CPU 3.4GHz (32GB RAM) using Magma V2.19-9.

	$p = 2$				$p = 3$		
d	1	2	3	4	1	2	3
Degree	6	10	20	40	9	21	63
Average time	0.082s	0.77s	87.796s	2175.798s	0.166s	82.782s	2203.21s
Min/Max time			2s/315s	224s/8670s		46s/156s	510s/5906s

	$p = 5$		$p = 7$	$p = 11$
d	1	2	1	1
Degree	15	55	21	33
Average time	0.490s	48.4 hours	296.684s	2010.78s
Min/Max time		21.6 hours/116.3 hours		1208s/4009s

Table 9.1

Index of Algorithms

Bibliography

[Art65] E. Artin, *The collected papers of Emil Artin*, Addison-Wesley, 1965.

[Bai96] G. Baier, *Zum Round 4 Algorithmus*, Master's thesis, Technische Universität Berlin, 1996.

[Bau14] Jens-Dietrich Bauch, *Lattices over polynomial rings and applications to function fields*, Ph.D. thesis, Universitat Autònoma de Barcelona, 2014.

[Ber05] Daniel J. Bernstein, *Factoring into coprimes in essentially linear time*, Journal of Algorithms **54** (2005), no. 1.

[BFH14] J.-F. Biasse, C. Fieker, and T. Hofmann, *Improvements on the computation of the hnf of a module over the ring of integers of a number field*, Submitted to Journal of Symbolic Computation, 2014.

[BL94] Johannes A. Buchmann and Hendrik W. Lenstra jr, *Approximating rings of integers in number fields*, Journal de Théorie des Nombres de Bordeaux **6** (1994), no. 2, 221–260.

[CBFS10] J. J. Cannon, W. Bosma, C. Fieker, and A. Steel (eds.), *Handbook of Magma functions (V2.17)*, Computational Algebra Group, University of Sydney, 2010, http://magma.maths.usyd.edu.au.

[CBFS13] J. J. Cannon, W. Bosma, C. Fieker, and A. Steel (eds.), *Handbook of Magma functions (V2.20)*, Computational Algebra Group, University of Sydney, 2013, http://magma.maths.usyd.edu.au.

[CH04] J. J. Cannon and D. F. Holt, *Computing the maximal subgroups of a finite group*, Journal of Symbolic Computation **37** (2004), 589–609.

[CH08] ———, *The transitive permutation groups of degree 32*, Experimental Mathematics **17** (2008), 307–314.

[Chi89] A. L. Chistov, *The complexity of constructing the ring of integers of a global field*, Soviet Mathematics Doklady (1989), 597–600, English translation.

[CLR90] Thomas H. Corman, Charles E. Leiserson, and Ronald L. Rivest, *Introduction to algorithms*, McGraw Hill, 1990.

[CM94] D. Casperson and J. McKay, *Symmetric functions, m-sets and Galois groups*, Mathematics of Computation **63** (1994), 749–757.

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Springer, 1993.

[Coh00] ———, *Advanced topics in computational number theory*, Springer, 2000.

[Dab95] M. Daberkow, *Über die Bestimmung der ganzen Elemente in Radikalerweiterungen algebraischer Zahlkörper*, Ph.D. thesis, Technische Universität Berlin, 1995.

[Dab01] ———, *On computations in Kummer extensions.*, Journal of Symbolic Computation **31** (2001), no. 1-2, 113–131.

[DF89] Henri Darmon and David Ford, *Computational verification of M_{11} and M_{12} as Galois groups over Q*, Communications in Algebra **17** (1989), 2941–2943.

[DF12] Virgile Ducet and Claus Fieker, *Computing equations of curves with many points*, ANTS X: Proceedings of the Tenth Algorithmic Number Theory Symposium (Everett Howe and Kiran Kedlaya, eds.), OBS, Mathematics Sciences Publishers, 2012.

[DS00] J.H. Davenport and G.C. Smith, *Fast recognition of symmetric and alternating Galois groups*, Journal of Pure and Applied Algebra **153** (2000), 17–25.

[Duv89] Dominique Duval, *Rational puiseux expansions*, Compositio Mathematica **70** (1989), 119 – 154.

[Eic96] Y. Eichenlaub, *Problémes effectifs de théorie de Galois en degrés 8 á 11*, Ph.D. thesis, Université Bordeaux I, 1996.

[Els12] A.-S. Elsenhans, *Invariants for the computation of intransitive and transitive Galois groups*, Journal of Symbolic Computation **47** (2012), 315–326.

[Els13a] ———, Personal communication, 2013.

[Els13b] ———, Personal communication, 2013.

[Els14a] ———, *A note on short cosets*, Experimental Mathematics **23** (2014), 411–413.

[Els14b] ———, *On the construction of relative invariants*, 2014.

[Fie02] C. Fieker, MAGMA implementation, V2.9, 2002.

[Fie06] ———, *Class theory of global fields*, Discovering Mathematics with Magma (J. J. Cannon and W. Bosma, eds.), Springer, 2006.

[Fie09] ———, Magma implementation and personal communication, 2009.

[Fie13a] ———, Personal communication, 2013.

[Fie13b] ———, *Algorithmic number theory, Lecture notes for winter 2103/14, TU-Kaiserslautern*, 2013.

[FK14] C. Fieker and J. Klüners, *Computation of Galois groups of rational polynomials*, London Mathematical Society Journal of Computation and Mathematics **17** (2014), no. 1, 141 – 158, http://arxiv.org/abs/1211.3588.

[FL94] D. Ford and P. Letard, *Implementing the round four maximal order algorithm*, Journal de Théorie des Nombres de Bordeaux (1994), no. 6, 39–80, http://almira.math.u-bordeaux.fr:80/jtnb/1994-1/jtnb6-1.html.

[Fra05] R. Fraatz, *Computation of maximal orders of cyclic extensions of function fields*, Ph.D. thesis, Technische Universität Berlin, 2005.

[Gei03] K. Geißler, *Berechnung von Galoisgruppen über Zahl- und Funktionenkörpern*, PhD Thesis, Technische Universität Berlin, 2003, available at URL:http://www.math.tu-berlin.de/˜kant/publications/diss/geissler.pdf.

[GG02] The GAP Group, *Gap – groups, algorithms, and programming, version 4.3*, 2002.

[GK00] K. Geißler and J. Klüners, *Galois group computation for rational polynomials*, Journal of Symbolic Computation **30** (2000), no. 6, 653–674.

[GMN11] J. Guàrdia, J. Montes, and E. Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, Journal de Théorie des Nombres de Bordeaux **23** (2011), no. 3, 667–696.

[GMN12] ———, *Newton polygons of higher order in algebraic number theory*, Transactions of the American Mathematical Society **364** (2012), no. 1, 361–416.

[GMN13] ———, *A new computational approach to ideal theory in number fields*, Foundations of Computational Mathematics **13** (2013), 729–762.

[Has80] H. Hasse, *Number theory*, Springer Verlag, 1980.

[Heß99] Florian Heß, *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern*, PhD Thesis, Technische Universität Berlin, 1999, URL:http://www.math.tu-berlin.de/∼kant/publications/diss/diss_FH.ps.gz.

[Hop98] A. Hoppe, *Normal forms over Dedekind domains – efficient implementation in the computer algebra system KANT*, Ph.D. thesis, Technische Universität Berlin, 1998.

[Hul99] Alexander Hulpke, *Galois groups through invariant relations*, Groups St. Andrews 1997 in Bath. Selected papers of the international conference, Bath, UK, July 26–August 9, 1997 (Cambridge) (C. M. Campbell et al, ed.), vol. 2, Lond. Math. Soc. Lect. Note Ser., no. 261, Cambridge University Press, 1999, pp. 379–393.

[Hul05] Alexander Hulpke, *Constructing transitive permutation groups*, Journal of Symbolic Computation **39** (2005), no. 1, 1–30. MR 2168238

[KM] J. Klüners and G. Malle, Database of polynomials over $\mathbb{Q}(t)$ with known Galois groups based on the polynomials in the appendix of [**MM99**].

[Knu97] Donald E. Knuth, *The art of computer programming, Volume 1, Fundamental algorithms*, Addison Wesley, 1997.

[Mar77] D. A. Marcus, *Number fields*, Springer-Verlag, 1977.

[MM97] T. Mattman and J. McKay, *Computation of Galois groups over function fields*, Mathematics of Computation **66** (1997), 823–831.

[MM99] G. Malle and B.-H. Matzat, *Inverse Galois theory*, Springer, 1999.

[Pau01] S. Pauli, *Factoring polynomials over local fields*, Journal of Symbolic Computation **32** (2001), 533–547.

[Poh94] M. Pohst, *In memoriam : Hans Zassenhaus*, Journal of Number Theory **47** (1994), 1–19.

[Poh96] ———, *Computational aspects of Kummer theory*, Cohen, Henri (ed.), Algorithmic number theory. Second international symposium, ANTS-II, Talence, France, May 18-23, 1996. Proceedings. Berlin: Springer. Lecture Notes Computer Science 1122, 259-272 (1996)., 1996.

[PZ89] M. Pohst and H. Zassenhaus, *Algorithmic algebraic number theory*, Cambridge University Press, 1989.

[Ser88] J.-P. Serre, *Algebraic groups and class fields*, Springer-Verlag, 1988.

[Ser03] Ákos Seress, *Permutation group algorithms*, Cambridge University Press, 2003.

[SM85] L. Soicher and J. McKay, *Computing Galois groups over the rationals*, Journal of Number Theory **20** (1985), 273–281.

[Soi81] L. Soicher, *The computation of Galois groups*, Master's thesis, Concordia University, Montreal, 1981.

[SS71] Arnold Schönhage and Volker Strassen, *Schnelle Multiplikation großer Zahlen*, Computing **7** (1971), no. 3-4, 281–292.

[Sta73] Richard P. Stauduhar, *The determination of Galois groups*, Mathematics of Computation **27** (1973), 981–996.

[Sti93] H. Stichtenoth, *Algebraic function fields and codes*, Springer–Verlag, 1993.

[Sut12] N. Sutherland, *Efficient computation of maximal orders in radical (including Kummer) extensions*, Journal of Symbolic Computation **47** (2012), 552–567.

[Sut13] ———, *Efficient computation of maximal orders in Artin–Schreier extensions*, Journal of Symbolic Computation **53** (2013), 26–39.

[Sut14] ———, *Efficient computation of maximal orders in Artin–Schreier–Witt extensions*, Submitted to Journal of Symbolic Computation, 2014.

[Sut15] ———, *Computing Galois groups of polynomials (especially over function fields of prime characteristic)*, Journal of Symbolic Computation **71** (2015), 73–97.

[Tig01] Jean-Pierre Tignol, *Galois' theory of algebraic equations*, World Scientific, 2001.

[vdW66] B. L. van der Waerden, *Modern algebra*, Frederick Ungar Publishing Co., 1966.

[vHKN11] M. van Hoeij, J. Klüners, and A. Novocin, *Generating subfields*, ISSAC 2011, 2011.

[Wit36] E. Witt, *Zyklische Körper und Algebren der Charakteristik p vom Grad p^n*, Journal für die reine und angewandte Mathematik **176** (1936), 126–140.

[Yok97] K. Yokoyama, *A modular method for computing Galois groups of polynomials*, Journal of Pure and Applied Algebra **117–118** (1997), 617–636.